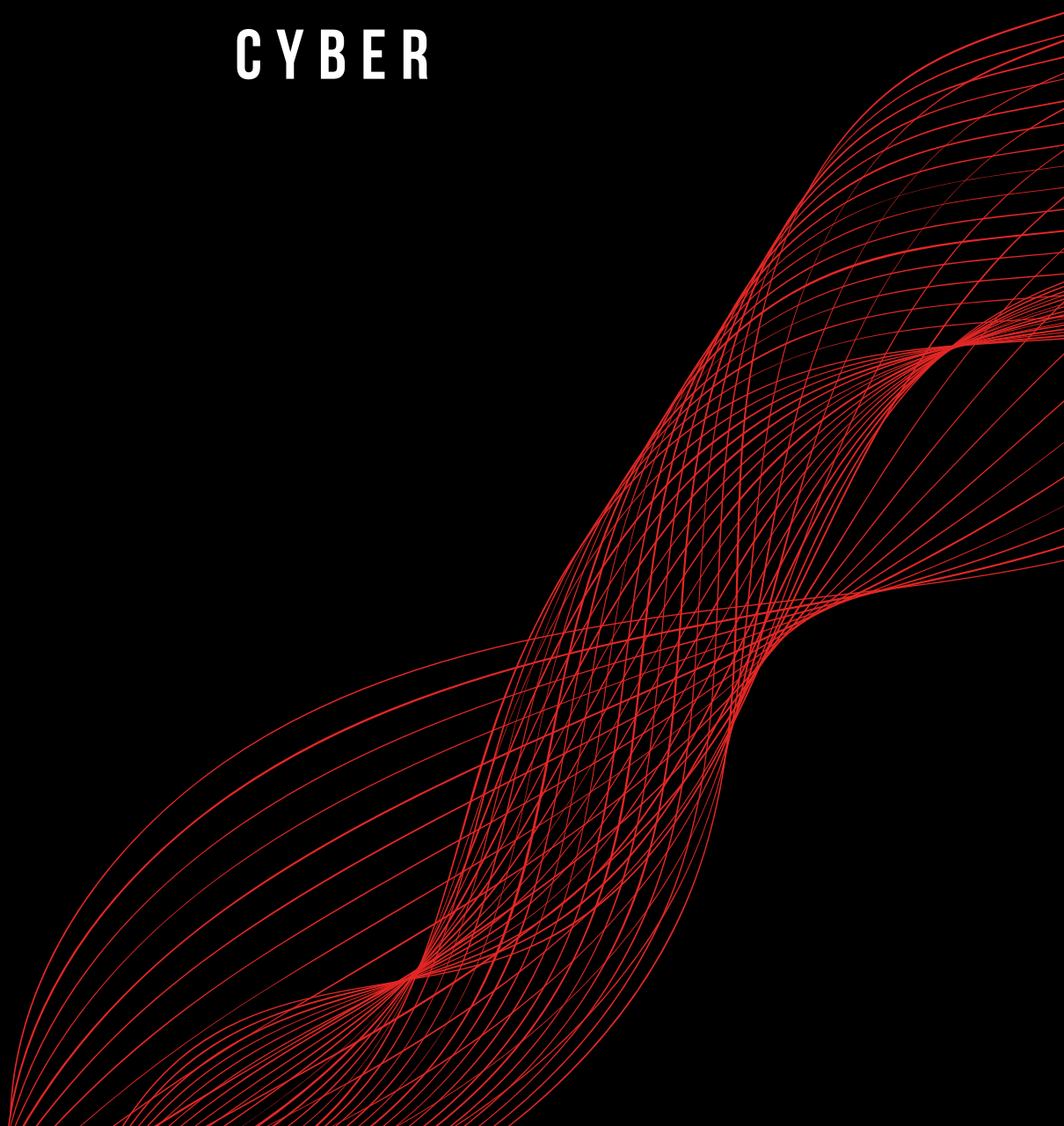
GoSec 24

TABLE RONDE CISO : LEADERSHIP EN CYBERSÉCURITÉ À L'ÈRE DE L'IA ET DE L'ASSURANCE CYBER



GoSec 24

Table ronde CISO

Résumé Exécutif

Le 12 septembre 2024, lors de GoSec24 à Montréal, une table ronde a offert une plateforme aux CISO et aux leaders en cybersécurité pour échanger des idées et des expériences. Ce livre blanc se concentre sur les défis posés par l'intégration des technologies d'IA, le rôle évolutif de l'assurance cyber, l'importance croissante de la résilience en cybersécurité, et les complexités du maintien de la vie privée. En s'appuyant sur des perspectives issues de divers secteurs, les idées des CISO enrichissent la réflexion sur des stratégies pratiques et des meilleures pratiques pour gérer ces défis tout en maintenant la résilience organisationnelle. Alors que les risques en cybersécurité continuent de croître, la nécessité d'une gouvernance claire, d'une gestion efficace des ressources et de stratégies de réponse aux incidents solides devient de plus en plus urgente.

Introduction

La complexité des défis en matière de cybersécurité auxquels les organisations sont confrontées continue de croître. Pour favoriser une plateforme où les organisations peuvent discuter ouvertement de leurs défis de sécurité et partager des solutions, GoSecure a organisé la Table ronde des CISO lors de l'événement GoSec24 à Montréal, le 12 septembre 2024. La table ronde a réuni 19 CISO et leaders de divers secteurs, dont les services financiers, la fabrication et les infrastructures publiques. Leurs années d'expérience en tant que leaders allaient de 5 à 20 ans. La diversité des tailles d'organisations et des expériences des CISO a enrichi les discussions, apportant une profondeur et une perspective précieuses.

La table ronde était modérée par le CTO de GoSecure et s'est tenue sur place dans une salle privée. La session offrait un cadre exclusif pour des discussions approfondies et permettait aux CISO de discuter ouvertement de sujets clés comme la gouvernance de l'IA, le rôle de l'assurance cyber, et l'intégration de la résilience dans les programmes de cybersécurité. Ce livre blanc met en lumière les thèmes clés de la discussion, fournissant des idées actionnables pour aider les CISO à naviguer à travers ces enjeux pressants. La discussion était guidée par trois questions principales, couvrant un éventail de sujets allant du rôle évolutif de l'assurance cyber et son impact sur les programmes de cybersécurité, aux défis de la protection de la vie privée et de la gestion de l'utilisation de l'IA. Les questions qui ont structuré la conversation se trouvent en annexe.

GoSec 24

Table ronde CISO

Points Saillants

Résumé des points saillants de la discussion

- **Coûts et efficacité de l'assurance cyber** – Malgré les primes élevées et les limitations de couverture perçues, discutées par plusieurs CISO, l'assurance cyber est reconnue comme nécessaire dans certains secteurs. De nombreuses organisations envisagent désormais également des alternatives telles que l'auto-assurance et l'amélioration de leurs stratégies de gestion des risques pour répondre aux exigences évolutives des assureurs.
- **Conformité et risques partenaires dans l'assurance cyber** – Alors que les organisations sont confrontées à des exigences de conformité étendues de la part des assureurs, ces exigences renforcent l'application de politiques rigoureuses non seulement en interne mais aussi parmi les partenaires pour sécuriser la couverture d'assurance. Dans les industries réglementées, où le maintien de la crédibilité et de la confiance est primordial, il reste essentiel de respecter les meilleures pratiques, y compris des révisions régulières des politiques et l'intégration de services de réponse aux brèches.
- **Changement de mentalité des CISO et accent sur le risque** – La résilience cyber est devenue une priorité clé pour les organisations après la pandémie, conduisant les CISO à adopter une mentalité plus consciente des risques. Ils sont désormais plus rigoureux dans l'évaluation des options de services et privilégient une protection complète, soulignant la nécessité d'un cadre de réponse aux incidents robuste, incluant une communication claire avec les parties prenantes en cas d'incidents de cybersécurité.
- **Accent sur la préparation et la formation à la résilience** – Les organisations doivent non seulement être prêtes à répondre aux incidents, mais aussi maintenir la continuité opérationnelle. Cela inclut l'utilisation de solutions cloud pour la protection des données et la conduite régulière d'exercices de réponse aux incidents impliquant à la fois les équipes techniques et la participation plus large de l'organisation. Des programmes de formation continue sont essentiels pour cultiver une culture de résilience où la cybersécurité est considérée comme une responsabilité partagée à tous les niveaux.
- **Défis de la gouvernance de l'IA** – Les CISO expriment des préoccupations concernant l'intégration rapide de l'IA au sein des organisations, la considérant comme un possible frein aux politiques et à la gouvernance. Les CISO sont incités à évaluer de manière critique la nécessité de certaines applications d'IA, en veillant à ce qu'elles répondent aux besoins des départements.
- **Solutions d'intégration de l'IA** – L'essor de l'IA nécessite des cadres de gouvernance robustes pour protéger les données sensibles et les secrets d'entreprise. Cela peut inclure le développement de solutions d'IA internes et l'intégration de clauses strictes dans les contrats avec les partenaires pour gérer les risques liés à l'IA. Une approche proactive est essentielle, mettant l'accent sur l'établissement de politiques formelles pour l'utilisation de l'IA. Une formation complète des employés est également nécessaire pour atténuer les risques et sensibiliser aux opportunités et menaces liées à ces technologies.

Cyber-assurance : Évaluer son impact comme soulagement ou fardeau

L'assurance cyber est devenue un élément bien établi des stratégies de gestion des risques des organisations. Plusieurs défis et frustrations ont été soulevés concernant l'assurance cyber. Premièrement, le processus de conclusion des contrats d'assurance exige des ressources organisationnelles importantes. Par exemple, certains CISO ont dû affecter plusieurs membres du personnel à plein temps pendant plusieurs mois juste pour naviguer à travers les questionnaires étendus et complexes. Les CISO ont également souligné le manque de soutien et d'outils fournis pour les aider dans ce processus.

Deuxièmement, si une organisation parvient à remplir toutes les exigences strictes imposées par les assureurs, la question se pose de savoir si l'assurance est toujours nécessaire. À ce stade, l'entreprise peut avoir déjà atteint un niveau de sécurité et de résilience qui rend inutile une telle couverture.

Troisièmement, les primes sont souvent élevées, et dans certains cas, un seul assureur peut ne pas fournir la couverture requise, obligeant les entreprises à traiter avec plusieurs assureurs, ce qui augmente la complexité.

Le quatrième défi lié à l'assurance cyber est que les organisations doivent désormais incorporer des règles et des politiques rigoureuses non seulement pour elles-mêmes, mais aussi pour leurs partenaires afin de se conformer aux contrats d'assurance et aux obligations. Par conséquent, les partenaires peuvent potentiellement représenter une menace pour la couverture d'assurance d'une organisation.

Enfin, au-delà des ressources et des coûts, un autre problème majeur est la longue liste d'exigences de conformité imposées par les assureurs. La question devient non pas de savoir si vous voulez être assuré, mais si c'est même faisable dans votre situation.

Bien que des préoccupations aient été soulevées concernant les primes élevées et la couverture incohérente offerte par les assureurs, l'assurance cyber reste vitale, en particulier dans les secteurs où elle est requise par contrat. L'objectif de souscrire une assurance cyber est parfois orienté vers le maintien de la crédibilité vis-à-vis des clients, mais il a été souligné que la couverture peut parfois ne pas offrir une valeur ajoutée significative. En d'autres termes, cette pression externe renforce le besoin pour de nombreuses organisations de conserver des politiques d'assurance, car elles servent de marqueur de confiance et de préparation aux yeux des clients et des partenaires.

Les meilleures pratiques pour maximiser la valeur de l'assurance cyber incluent la révision régulière des politiques, le travail avec des courtiers expérimentés et l'assurance que la couverture répond aux risques actuels et futurs. Les CISO ont également recommandé d'intégrer des coachs en violation de données et des services de réponse aux incidents dans ces politiques pour mieux se préparer aux incidents et minimiser les temps d'arrêt opérationnels lors d'une cyberattaque.

L'approche axée sur la résilience

La résilience cyber est devenue une priorité cruciale dans le paysage post-pandémique, définie comme la capacité d'une organisation à prévenir, supporter et se remettre des incidents de cybersécurité. Les CISO ont noté que ce changement a fondamentalement modifié leur approche et leur état d'esprit envers leurs rôles. Ils sont devenus de plus en plus conscients des risques, les amenant à adopter une approche plus rigoureuse et plus inquisitive lorsqu'ils évaluent les options de services, posant des questions plus détaillées pour garantir une protection complète.

Le besoin d'un cadre complet de réponse aux incidents a été un thème récurrent. Au-delà de la récupération technique, les organisations doivent également donner la priorité à une communication claire et transparente avec les parties prenantes et les clients en cas de violation de données. Si les données des clients sont affectées, la récupération de la réputation devient tout aussi cruciale que la récupération opérationnelle, car perdre la confiance des clients peut avoir des effets durables sur l'entreprise. Le maintien de la confiance est essentiel, surtout lorsqu'il s'agit de données sensibles. Les discussions de la table ronde ont souligné l'importance de développer une approche axée sur la résilience, garantissant que les organisations ne sont pas seulement prêtes à répondre aux incidents, mais qu'elles peuvent continuer à fonctionner avec un minimum de perturbations. Il a été recommandé de tirer parti des solutions basées sur le cloud offrant redondance et évolutivité comme moyen de protéger les données critiques, garantissant que les entreprises puissent se remettre rapidement des incidents.

La résilience repose également sur des tests réguliers des plans de réponse aux incidents. Les CISO ont plaidé en faveur d'exercices fréquents impliquant à la fois les équipes techniques et une participation plus large de l'organisation, afin de s'assurer que tous les niveaux de l'entreprise soient préparés à faire face aux menaces cyber. Cette approche holistique devrait s'étendre au-delà du département informatique, avec une sensibilisation à la cybersécurité intégrée dans tous les aspects des opérations commerciales. L'inclusion de programmes d'éducation continue pour les employés à tous les niveaux aide les organisations à bâtir une culture plus résiliente, où la sécurité est une responsabilité partagée.

Les CISO restent prudents face à la frénésie autour de l'IA

L'intégration rapide de l'IA dans le paysage organisationnel a été jugée préjudiciable par les CISO en ce qui concerne les politiques et la gouvernance. Bien que leur instinct les ait poussés à freiner son adoption, la crainte pressante de prendre du retard par rapport aux concurrents — qui adoptent tous ces outils — a rendu cette option de plus en plus difficile à maintenir.

Au milieu de l'engouement pour l'IA, les CISO sont obligés de se poser des questions fondamentales. Par exemple, bien qu'il y ait un intérêt à intégrer des outils comme Copilot, ils doivent évaluer si ces outils sont vraiment nécessaires dans tous les départements. Bien que Copilot puisse être très utile pour les ventes, il pourrait ne pas être aussi pertinent pour d'autres domaines. Par conséquent, pour des raisons de sécurité et afin de naviguer efficacement dans cet engouement, il est essentiel que les CISO comprennent pleinement les outils disponibles, leurs utilisations prévues, et qu'ils sachent affirmer quand certaines solutions d'IA peuvent être inutiles.

Le rôle du CISO est non seulement influencé par les préoccupations en matière de sécurité liées à l'IA, mais aussi considérablement affecté par les questions de confidentialité des données soulevées par ces technologies. Les CISO soulignent la nécessité d'obtenir des conseils pour intégrer l'IA de manière sécurisée. Ils reconnaissent l'impératif de protéger les informations personnelles ainsi que les secrets de l'entreprise. Cette situation a conduit certaines organisations à envisager de développer des solutions d'IA internes pour alléger les charges associées.

Similaire aux défis posés par l'assurance cyber, les partenariats organisationnels présentent des risques supplémentaires en ce qui concerne l'IA. Bien que les CISO puissent mettre en place des politiques internes robustes, ils doivent également envisager d'intégrer des clauses strictes dans les contrats de partenariat qui obligent à une gestion rigoureuse de l'IA en relation avec les informations internes. Il est crucial de s'assurer que les limites établies soient respectées par toutes les parties impliquées.

Les CISO ont souligné l'importance d'adopter une approche proactive et structurée de la cybersécurité, surtout à mesure que des technologies émergentes comme l'IA deviennent une partie intégrante des opérations quotidiennes. Les discussions ont mis en évidence la nécessité de cadres de gouvernance robustes autour de l'utilisation de l'IA, garantissant que les organisations puissent tirer parti de ces technologies sans exposer de données sensibles ni compromettre les normes de sécurité.

L'établissement de politiques formelles sur l'utilisation de l'IA a été souligné comme une étape fondamentale, et la deuxième solution importante soulevée est la formation des employés. La première est cruciale pour s'assurer que le personnel comprenne à la fois les opportunités et les risques associés à l'IA. Les programmes de formation complets atténuent non seulement les risques comme les fuites de données, mais aident également les employés à reconnaître les accès non autorisés à des informations propriétaires.

Conclusion

Lors de la table ronde des CISO, il devient évident qu'une approche holistique et intégrée, caractérisée par la mutualisation, qui permet un apprentissage continu et une adoption plus rapide des avancées technologiques, est la voie à suivre vers un avenir plus collaboratif et efficace pour la cybersécurité. À mesure que les menaces évoluent, nos stratégies et pratiques doivent également s'adapter. Ce livre blanc souligne la sagesse collective des vétérans de l'industrie et sert de phare pour les organisations cherchant à renforcer leurs cadres de cybersécurité.

GoSec 24

Table ronde CISO

Annexe

Questions clés discutées

Question 1 : L'assurance cyber a subi de nombreux changements depuis son arrivée sur le marché, passant d'une grande instabilité (avec des changements majeurs d'une année à l'autre) à une stabilisation, selon certaines sources, au cours des deux dernières années.

- Comment le besoin d'une assurance cyber a-t-il affecté votre organisation ?
- Considérez-vous cela comme un avantage ou un obstacle pour le programme de cybersécurité que vous avez mis en place ?
- Avez-vous reçu des demandes déraisonnables de la part de vos assureurs ?

Question 2 : La résilience cyber est devenue un sujet brûlant dans le monde post-pandémique. Elle peut être définie comme la capacité d'une organisation à prévenir, supporter et se remettre des incidents de cybersécurité.

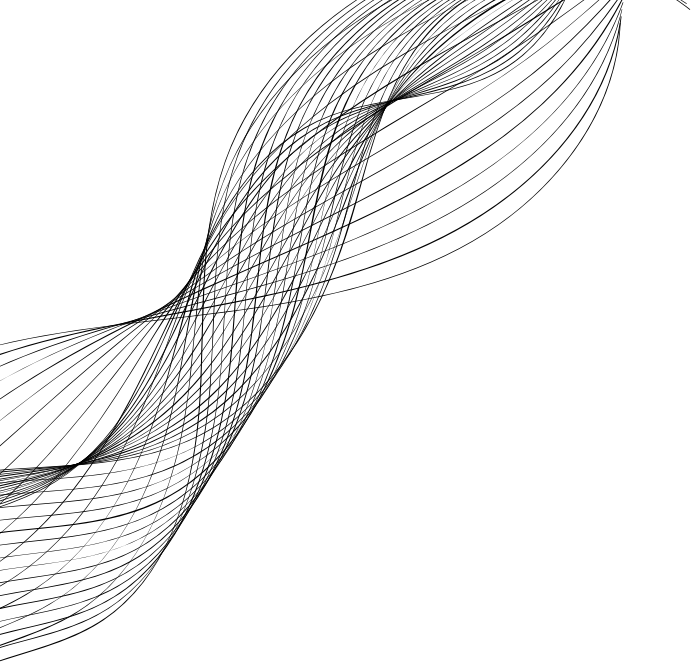
- Votre organisation a-t-elle adopté ce concept ?
- Comment cela a-t-il modifié votre approche ?
- Y a-t-il des "leçons" de la pandémie qui ont amélioré les choses pour votre organisation ?

Question 3a : En ce qui concerne la confidentialité, en tant que responsable de la cybersécurité dans votre organisation,

- Surveillez-vous vos employés et est-ce éthique de le faire ?
- Avec de nombreux employés qui utilisent leurs ordinateurs de travail à des fins personnelles, où se situe la limite en matière de confidentialité de vos utilisateurs ?
- Vous préoccupez-vous de ce que les gens publient sur les réseaux sociaux (puisqu'une partie de cela peut être liée à l'organisation) ? Si oui, comment abordez-vous cela ?
- Avez-vous été confronté à la publication d'informations sensibles ?

Question 3b : Dans cette même optique, de plus en plus d'utilisateurs utilisent l'IA/ChatGPT pour écrire, traduire, interpréter.

- Que faites-vous pour empêcher que des informations sensibles ne soient fournies au prestataire LLM ?
- Votre organisation a-t-elle une position formelle à ce sujet ? Ou faites-vous simplement confiance au fournisseur ?



Organisateur :

Julien Turcot est le vice-président principal des ventes chez GoSecure et il est basé à Québec.

L’auteur souhaite remercier GoSecure et les CISO pour leurs contributions à la table ronde.