Institut des Administrateurs de Sociétés

La transcription de la baladodiffusion : Il est résolu que les conseils d'administration doivent repenser fondamentalement les cyberrisques à l'ère de l'IA.

Rahul Bhardwaj (00:04): Bienvenue à la baladodiffusion Be It Resolved, qui est le point de rencontre entre des idées audacieuses et un leadership courageux. Je suis votre hôte, Rahul Bhardwaj. Je suis président et chef de la direction de l'Institut des administrateurs de sociétés du Canada. Dans chaque épisode, je m'entretiendrai avec des experts pour étudier à fond des questions urgentes qui ont une incidence sur les administrateurs et la prise de décision dans la salle du conseil.

Aujourd'hui, mon invité est Stephen Burns, associé du cabinet d'avocats Bennett Jones S.E.N.C.R.L./s.r.l. et coprésident du groupe Technologie et propriété intellectuelle du cabinet. Son travail porte sur le droit des technologies, y compris la gouvernance des données, la cybersécurité, la protection de la vie privée et la propriété intellectuelle. Il comparaît régulièrement devant les commissaires à l'information et à la protection de la vie privée du Canada et publie sur des sujets clés, tels que l'IA et les cyberrisques.

Aujourd'hui, Steven nous fera part de ses réflexions sur la nécessité de considérer la cybersécurité comme une priorité stratégique à part entière pour les conseils d'administration. Il en profitera également pour nous expliquer le phénomène connu sous le nom d'« effet pastèque ». J'ai hâte d'en savoir plus.

La résolution d'aujourd'hui est la suivante : il est résolu que les conseils d'administration doivent repenser fondamentalement les cyberrisques à l'ère de l'IA.

Bienvenue Stephen. Ravi de vous avoir parmi nous aujourd'hui.

Stephen Burns (01:14): Merci. Je suis très heureux d'être ici.

Rahul Bhardwaj (01:16): Nous parlons ici de l'évolution des cyberrisques. Pour ceux qui ne sont pas très familiers avec le sujet, que signifie exactement le terme « cyberrisque », et plus particulièrement dans le cadre de la salle du conseil?

Stephen Burns (01:28): C'est un excellent point de départ, et je pense que c'est très important quand on commence à parler de cyberrisque. Il est facile de se perdre dans la multitude de cyberattaques possibles, d'outils et de méthodes employées. Je pense, dans le cadre des conseils d'administration, qu'il est préférable de prendre du recul et de considérer d'abord ce qu'on cherche à protéger : les renseignements que l'organisation recueille, utilise et analyse pour maintenir son avantage concurrentiel et assurer la distribution de ses produits et services. Ces renseignements sont souvent propres à l'organisation et revêtent une grande valeur.

La deuxième catégorie à protéger concerne les actifs opérationnels de l'organisation, ceux qui dépendent de systèmes électroniques ou informatiques. Cela peut être, par exemple, les systèmes de contrôle d'un pipeline ou bien d'une machine qui fabrique un certain produit.

Quand on considère que l'objectif est de protéger à la fois les renseignements de l'organisation et ses technologies opérationnelles, il devient essentiel d'examiner les facteurs qui garantissent cette protection. Dispose-t-on de contrôles physiques, procéduraux et techniques adéquats? J'ajouterais à cela un quatrième élément : des contrôles de gestion suffisants au niveau du conseil d'administration afin de s'assurer que toutes les protections physiques, techniques et procédurales sont bien prises en compte en fonction des risques propres aux renseignements ou aux actifs opérationnels, ainsi que des évolutions technologiques susceptibles d'impacter la sécurité. Je crois que cela prépare bien le terrain pour la suite de notre discussion.

Ensuite, il s'agit d'analyser la conception du système concerné, la valeur des renseignements qu'il traite, et la façon dont l'organisation va faire évoluer ce système d'information ou opérationnel afin d'exploiter les nouvelles capacités offertes par l'intelligence artificielle, soit de nouveaux outils qui permettent une meilleure compréhension des données, un contrôle renforcé des opérations, et, en fin de compte, une création de valeur accrue pour l'entreprise.

Rahul Bhardwaj (03:50): La résolution d'aujourd'hui concerne surtout un changement potentiel avec l'arrivée de l'IA, sans pour autant minimiser le travail déjà accompli par les administrateurs dans ce domaine. Parlons-en un peu. Qu'est-ce qui a changé pour que les administrateurs aient confiance en leur capacité de surveillance dans ce domaine?

Stephen Burns (04:06): Beaucoup d'efforts ont été consacrés à former les conseils d'administration et à leur fournir les connaissances nécessaires afin qu'ils posent les bonnes questions. Ils cherchent à comprendre où se trouvent leurs données, si elles sont sécurisées, si elles sont fiables, la manière dont leurs opérations sont protégées et s'il existe un risque significatif qu'une partie de leurs activités soit interrompue ou subisse un impact majeur s'ils sont incapables de les utiliser. Ces préoccupations découlent de la structure même des systèmes d'information et opérationnels.

Traditionnellement, la protection des systèmes passait souvent par leur isolement complet – ce qu'on appelle un isolement physique – en les maintenant comme des systèmes autonomes. Puis, les systèmes étaient peu interconnectés : les données des ressources humaines, par exemple, étaient stockées dans des systèmes séparés de ceux des données financières ou des données clients. Ces approches ont changé : on reconnaît aujourd'hui la valeur des données et on les rassemble dans de grands lacs de données afin d'analyser et de comprendre les activités de l'organisation dans l'ensemble, plutôt que de manière fragmentée, système par système.

Le regroupement des systèmes et la centralisation des données ont fait disparaître la protection qu'offrait la fragmentation. De petits systèmes discrets, autrefois peu attrayants, ont laissé place à de vastes ensembles de données, attirant l'attention de cybercriminels, d'activistes ou même d'acteurs étatiques. En cherchant à mieux exploiter nos propres ressources, nous les avons aussi rendues plus précieuses et donc plus attractives pour les auteurs de menace.

Rahul Bhardwaj (05:47): Ce changement semble être une arme à double tranchant. Avant de passer à la question de l'IA, dans le cadre du modèle en place jusque-là, qui était responsable de la surveillance des cyberrisques? Puis, plus précisément au sein du conseil d'administration, est-ce que cette responsabilité relevait principalement du comité de vérification?

Stephen Burns (06:04): En fin de compte, la responsabilité incombe toujours au conseil d'administration. Toutefois, cette responsabilité est souvent déléguée, soit au comité de vérification, soit directement à l'équipe de direction. De nombreuses organisations ont vu leur chef de la direction nommer un directeur des technologies de l'information (DPI), puis, plus récemment, un directeur de la sécurité de l'information. Ainsi, un membre de l'équipe de direction est désigné pour comprendre l'emplacement des données, pour repérer les menaces, pour déterminer les zones vulnérables et pour allouer les ressources de manière stratégique.

Je pense qu'il est important de préciser, en passant, que la cybersécurité engendre des coûts importants et qu'il n'est pas pertinent d'appliquer les mêmes niveaux de protection à tout. Une évaluation des risques permet de déterminer les renseignements les plus précieux et les opérations les plus importantes, ainsi que leur protection, afin d'investir les ressources de manière judicieuse.

C'est généralement à ce niveau que les conseils d'administration intervenaient pour s'assurer d'avoir une stratégie de cybersécurité en place, à la fois efficace et économiquement raisonnable, avec des responsables compétents au sein de l'organisation. La plupart des entreprises cherchaient à bien gérer la sécurité sans pour autant dépenser excessivement pour un risque considéré comme essentiellement théorique. Les cyberattaques étaient peu fréquentes, ou du moins beaucoup moins nombreuses qu'aujourd'hui, 15 ans plus tard.

Rahul Bhardwaj (07:38): Nous en avons déjà parlé : les conseils d'administration ont le devoir d'agir dans l'intérêt de leur société. Ils assurent la surveillance de la culture, de la stratégie et des risques. Comme les données sont perçues, dans le cas de nombreuses sociétés, comme les actifs attrayants de la société, les conseils d'administration les considèrent selon une perspective du risque. Or, j'ai l'impression qu'avec l'essor de l'IA, vous semblez suggérer un changement de perspective qui passerait d'une gestion des risques à une approche plus stratégique. Explorons ce point plus en détail. Pouvez-vous expliquer un peu plus ce que vous entendez par là?

Stephen Burns (08:08): Cela fait des décennies que l'intelligence artificielle est présente, sous diverses formes, dans les organisations. Plusieurs d'entre elles ont eu recours à l'apprentissage automatique pour évaluer les demandes de cartes de crédit ou pour décider de l'octroi d'un prêt. Plusieurs processus ont ainsi été automatisés afin d'exploiter les données de manière efficace.

Si l'on observe aujourd'hui une hausse marquée à la fois des menaces et des opportunités, c'est parce que certaines barrières ont été franchies. Ce fut le cas de la barrière linguistique il y a quelques années. Les grands modèles de langage ont commencé à comprendre le langage humain avec une précision qui rivalise – voire dépasse légèrement – celle des humains. Cela a ouvert la voie à toute une série de nouveaux outils capables d'analyser de vastes ensembles de données, révélant ainsi des perspectives très intéressantes.

L'intelligence artificielle n'a rien de magique. Ce n'est pas un outil unique capable de tout faire. Il s'agit plutôt d'un ensemble de technologies regroupées sous une même appellation, qui permet d'explorer les données en profondeur pour en extraire des perspectives pertinentes, d'analyser les opérations pour déterminer les manières d'alléger les coûts, et de mieux comprendre le fonctionnement global de l'entreprise.

Ce processus permet d'examiner les données d'une manière inédite grâce à ces outils. Il influence aussi la manière dont on aborde la gestion des cyberrisques où de grandes quantités d'informations sont regroupées dans des lacs ou des ensembles de données toujours plus vastes. Cela permet des analyses plus complètes et approfondies pour mieux comprendre. Toutefois, cela crée également des actifs attrayants plus importants et vulnérables face aux cyberattaques.

Rahul Bhardwaj (10:02): Vous avez mentionné précédemment qu'il y avait trois tsunamis – je crois que c'est le terme que vous avez employé – pour illustrer l'impact de l'IA sur l'environnement des cyberrisques.

Stephen Burns (10:14): Il y a, dans les faits, trois impacts macroéconomiques qui doivent être compris par les conseils d'administration. Quand on parle de technologie, on parle en réalité d'automatisation des processus opérationnels.

Il s'agit de réfléchir à la manière de réaliser efficacement les tâches nécessaires à la prestation des services ou produits de l'organisation sur le marché, en optimisant l'utilisation des ressources humaines et des technologies pour répondre aux attentes et aux besoins des clients.

Pour ce faire, on doit comprendre le fonctionnement de l'entreprise et les capacités offertes par la technologie. Ces deux éléments sont affectés par les trois tsunamis que nous observons actuellement.

Le premier phénomène est ce que l'on appelle le « tsunami gris » : les baby-boomers commencent à prendre leur retraite, entraînant une grande perte de savoir organisationnel. Ce qu'on constate, c'est que les entreprises n'ont généralement pas une compréhension très précise de la manière dont elles accomplissent les activités nécessaires pour mettre leurs produits et services sur le marché. Elles savent qu'elles le font, mais sans toujours savoir précisément comment cela se fait, et une partie importante de ce savoir s'en va avec les personnes qui partent à la retraite.

Le deuxième phénomène, c'est l'évolution rapide de la technologie. Autrefois, les ordinateurs étaient surtout utilisés pour effectuer des calculs simples, comme « deux plus deux égale quatre ». Ils n'étaient pas capables de traiter de grandes quantités de données pour en extraire de nouvelles perspectives. Aujourd'hui, grâce aux nouveaux modèles d'intelligence artificielle, il est possible d'analyser des quantités considérables de données et prédire des résultats d'une manière jusqu'à ce jour inédite. Cela transforme profondément la productivité et la qualité du travail accompli.

Les organisations sont très enthousiastes. Elles souhaitent adopter ces nouveaux outils, car elles sont convaincues qu'ils peuvent améliorer la qualité, accroître l'efficacité ou réduire les coûts, renforçant ainsi leur capacité concurrentielle sur le marché. En parallèle, les compétences nécessaires pour comprendre et exploiter ces outils quittent peu à peu l'entreprise avec les départs à la retraite, et la technologie, elle, évolue à toute vitesse. Ce décalage crée un véritable vide… et c'est ce qu'on appelle le troisième tsunami.

Le troisième tsunami est celui de la transformation. Les entreprises se voient contraintes de revoir leurs modes de fonctionnement, soit en raison du départ à la retraite, soit sous la pression des technologies émergentes. Nous traversons une période de bouleversements importants. C'est cette vague de transformation qui, à mon sens, constitue aujourd'hui le principal risque pour les conseils d'administration. Tout le monde sait qu'il faut en faire davantage et tirer parti de ces technologies. Ce qui demeure flou, c'est la manière d'y parvenir concrètement et de réussir cette transition. Malheureusement, les transformations organisationnelles échouent bien souvent.

Des études fiables montrent que, si les organisations gèrent assez bien les changements quotidiens, elles rencontrent beaucoup plus de difficultés lorsqu'il s'agit de transformations en profondeur, telles que restructurer l'entreprise, définir une stratégie, réfléchir à la mise en application de la stratégie et transformer l'organisation à l'aide de nouveaux outils adoptés pour mettre en œuvre la stratégie. Le taux de réussite de ces transformations est inférieur à 20 %. Parmi les 80 % d'échecs, environ 30 % à 40 % – soit la moitié – des projets aboutissent tout de même, mais à un coût multiplié par deux à cinq fois.

C'est cette pression constante qui pèse sur les conseils d'administration. Ils sont confrontés à de nouveaux outils et à de grandes quantités de données qu'ils souhaitent exploiter différemment. Ils savent que le savoir entourant le fonctionnement de l'entreprise s'en va avec les départs à la retraite, et que leurs concurrents vivent la même situation. Ils ne savent pas quoi faire.

Les conseils d'administration ne possèdent pas encore les compétences ni la clarté nécessaires pour interroger efficacement leur équipe de direction sur plusieurs points clés : « Comment est gérée la perte de savoir causée par le tsunami gris? Comment sont exploitées les nouvelles possibilités offertes par les technologies? Comment s'assurer d'être prêts, en tant que membres du conseil, à réaliser les meilleurs investissements dans les transformations requises, alors que nous ne savons pas comment évaluer notre réussite tout au long du processus? »

Rahul Bhardwaj (14:42): Il y a beaucoup d'informations à analyser avec ces trois tsunamis qui bouleversent tout. Pour les conseils d'administration, c'est une opportunité intéressante et séduisante, mais qui présente également une source de risque comme la concurrence s'y met aussi. Alors, dites-moi, selon vous, comment l'IA redéfinit-elle les cybermenaces?

Stephen Burns (15:04): Revenons un instant sur le modèle d'avant et comparons-le à celui d'aujourd'hui.

Avant, les systèmes étaient isolés et protégés de manière individuelle. Ils étaient souvent séparés les uns des autres de sorte qu'en cas d'attaque, les autres systèmes n'étaient pas touchés. Cet ancien modèle reposait sur des serveurs, des centres de données et des systèmes sous contrôle interne. Ce n'est plus le cas aujourd'hui. La cybersécurité est coûteuse, tout comme la protection des systèmes. Maintenir ces différents systèmes représente également d'importants coûts.

On observe un important mouvement vers l'infonuagique. Beaucoup d'organisations ont opté pour la simplification de leurs systèmes en les transférant vers des services basés sur l'infonuagique, confiant ainsi à des fournisseurs externes, notamment à des fournisseurs de services infonuagiques, des compétences et des connaissances autrefois gérées en interne. Cette évolution s'est faite naturellement. En regroupant les données dans un nuage partagé avec d'autres entreprises, on peut bénéficier d'économies d'échelle en répartissant les coûts liés à la sécurité.

Les outils qui permettent aux organisations d'exploiter leurs données de manière plus intelligente, d'avoir une meilleure compréhension de leurs activités et d'optimiser leurs services sont également à la disposition des auteurs de menace. Ces derniers les utilisent pour repérer plus efficacement les données ciblées, pour contourner les mesures de sécurité et pour affiner leur fraude psychologique et leurs stratégies d'attaque afin d'accéder aux mots de passe recherchés – et ils y parviennent.

Les gouvernements et les organisations des services de sécurité du monde entier tirent la sonnette d'alarme : ces nouveaux outils, entre de mauvaises mains, ouvrent la voie à des attaques d'un nouveau genre. Un exemple marquant : l'usage d'un avatar généré par l'intelligence artificielle a permis de convaincre un employé et son organisation d'autoriser des virements bancaires, parce qu'ils pensaient obéir à un cadre. L'intelligence artificielle est capable de combiner une voix, une vidéo et des informations pour persuader un employé d'une organisation de transférer de l'argent à des cybercriminels. Ce n'était pas possible il y a cinq ans, et ce l'est aujourd'hui grâce aux avancées de l'IA.

Rahul Bhardwaj (17:28): Les conseils d'administration entendent cette histoire alarmante et se disent : « Nous avons une équipe de direction compétente. Elle met en place des formations et des systèmes internes pour minimiser ces risques. » Puis, ils se demandent : « Comment savoir si nos meilleures pratiques sont adaptées? Nous pensions bien gérer le cyberrisque, mais l'IA change la donne. » Parlons un peu de ce point. Vous avez mentionné l'« effet pastèque » comme une piste intéressante pour guider les questions des administrateurs et des administratrices.

Stephen Burns (18:01): Commençons par expliquer l'« effet pastèque ».

L'« effet pastèque » fait référence à un tableau de bord ou à un système d'information de gestion qui affiche uniquement des indicateurs verts, que ce soit dans un système à trois ou à cinq couleurs – souvent vert, jaune et rouge – pour évaluer le profil de risque dans un rapport de gestion. En d'autres termes, les indicateurs clés de performance et les indicateurs de gestion sont affichés systématiquement en vert. Tout est vert jusqu'au jour où une attache survient, révélant que les indicateurs suivis n'étaient pas les bons. Le conseil d'administration et les systèmes de gestion s'appuyaient sur une évaluation du risque dépassée et les systèmes de gestion n'ont pas été mis à jour pour intégrer les risques actuels et émergents.

Si le système d'information de gestion affiche aujourd'hui le même tableau de bord qu'il y a cinq ans en ce qui concerne les risques liés à l'information et à la technologie, cela montre clairement qu'il n'a pas été mis à jour en temps opportun. Il n'affiche probablement pas la bonne information, et vous allez vous retrouver face à un « effet pastèque ».

Rahul Bhardwaj (19:18): Tout est vert à l'extérieur, mais en fait, c'est rouge à l'intérieur. Il y a un problème. Alors, si un administrateur ou une administratrice prend conscience de cet « effet pastèque » après avoir entendu Stephen Burns en parler et revient auprès de son conseil d'administration qui connaît également ce phénomène, comment peut-il ou peut-elle amorcer au sein du conseil une démarche pour éviter de tomber dans ce piège?

Stephen Burns (19:36): Je crois qu'il faut d'abord se demander où réside la valeur au sein de l'organisation et ce qu'il convient de sécuriser. La valeur d'une organisation repose généralement sur deux éléments : les ensembles de données qu'on souhaite exploiter et protéger contre une utilisation malveillante et l'infrastructure et les opérations, soit le fonctionnement interne, le fonctionnement des systèmes, ainsi que leur protection et leur fragmentation.

Après avoir identifié ce qu'on doit protéger, il faut réfléchir aux méthodes qui pourraient être employées pour les attaquer. Il faut envisager les méthodes d'attaque actuelles susceptibles de viser ces actifs. Comment un cybercriminel pourrait-il obtenir le contrôle de ces systèmes et y accéder? Ensuite, il faut examiner les mesures de protection en place. Quelles sont les mesures de protection physiques, procédurales et électroniques existantes? Il faut également se pencher sur les contrôles de gestion.

C'est une façon intéressante de voir les choses. Beaucoup d'outils d'IA générative sont gratuits. De nombreux systèmes que les employés souhaitent utiliser sont également gratuits ou peu coûteux, et ils peuvent facilement s'en servir en payant avec une carte de crédit au besoin. Autrefois, l'organisation associait le coût financier au niveau de risque et renforçait le contrôle à mesure que les dépenses augmentaient. Dans le cyberespace, cette approche ne fonctionne pas : les données les plus sensibles peuvent être compromises simplement parce qu'un employé souhaite tester un outil d'IA générative gratuit trouvé en ligne, dans l'espoir d'obtenir un résultat impressionnant à présenter à ses supérieurs. Or, justement parce que l'outil est gratuit, personne n'aura pris le temps de faire les vérifications nécessaires ni de se demander sérieusement si cet outil a réellement sa place dans l'organisation.

C'est un bon exemple des limites des mécanismes de contrôle traditionnels, fondés sur l'autorisation de dépenses et une hiérarchie basée sur les montants engagés. Dans l'univers technologique d'aujourd'hui, cette logique n'est pas adaptée, car beaucoup d'outils sont disponibles gratuitement ou à très faible coût.

Rahul Bhardwaj (21:54): Certains membres du conseil diront peut-être : « Nous avons ce risque sous contrôle. Des politiques et des procédures sont en place, elles sont respectées, et nous n'avons pas connu de cyberincident majeur jusqu'à présent. » Je suppose que vous leur répondriez que ce n'est pas suffisant dans le contexte actuel. Ils poseront alors la question suivante : « Que devons-nous changer? » Quelles seraient, selon vous, les premières mesures à mettre en œuvre? Et en ce qui concerne les compétences du conseil d'administration, faut-il repenser sa composition pour renforcer réellement sa capacité de surveillance?

Stephen Burns (22:22): Je ne suis pas en train de dire qu'il faut revoir entièrement la composition du conseil d'administration Ce serait une affirmation plutôt audacieuse. En revanche, je dirais qu'il y a un avantage à apporter une expertise technologique au sein du conseil ou à tout le moins dans ses échanges.

On observe aujourd'hui une tendance à intégrer des membres disposant d'une expertise technologique au sein des conseils d'administration. La richesse d'un conseil repose justement sur la diversité des parcours et des expériences que ses membres apportent aux échanges. C'est pourquoi ajouter une voix forte en matière de technologie ne peut qu'aider.

Le deuxième point que les conseils d'administration examinent de près, c'est la compétence technologique au sein de l'équipe de direction. Ils veulent savoir si leur équipe de la haute direction est non seulement consciente des risques stratégiques – comme ceux dont nous parlons – mais aussi de l'importance stratégique des nouvelles technologies. Cela implique de comprendre où ces technologies peuvent réellement créer de la valeur pour l'organisation et comment les exploiter pour renforcer sa position concurrentielle grâce à des investissements ciblés.

Parfois, il n'est pas judicieux de réaliser un investissement important, par exemple dépenser 4 millions de dollars pour économiser seulement 100 000 dollars dans un processus opérationnel. Ce qui n'est pas un choix rentable. En revanche, un investissement de quelques centaines de milliers dans un outil qui améliore la productivité de 20 %, tout en améliorant la qualité et la rapidité du travail des équipes, devient une décision tout à fait pertinente.

Le deuxième point sur lequel les conseils d'administration doivent agir, c'est revoir leurs mécanismes de contrôle des risques pour s'assurer qu'ils sont bien adaptés au nouvel environnement. Un bon exemple de cette adaptation est l'approche adoptée par certaines organisations concernant la gestion des données : elles classent leurs données en cinq ou six catégories, puis déterminent, pour chacune de ces catégories, le niveau d'autorité requis avant que les données puissent être intégrées à un nouveau système.

Ainsi, lorsqu'une donnée appartient à une catégorie hautement sensible, la décision d'utiliser un logiciel ne peut plus reposer uniquement sur son prix, par exemple : « Ce logiciel ne coûte que 100 dollars, donc je peux l'utiliser sans autorisation. » Même si le logiciel ne coûte que 100 dollars, si les données concernées relèvent d'une catégorie 5, il faut obtenir la signature d'un vice-président avant que de pouvoir les utiliser. Les organisations commencent ainsi à adapter leurs mécanismes de contrôle en fonction du niveau de risque.

Rahul Bhardwaj (24:51): On en vient à comprendre que ce qui nous a permis d'arriver là où nous sommes aujourd'hui ne nous mènera pas forcément plus loin. Les conseils d'administration doivent sans cesse revoir et repenser leur approche afin de pouvoir anticiper les nouveaux risques et saisir les opportunités stratégiques qui se présentent. Cela dit, il semble étrange de parler des cyberrisques sans aborder le sujet incontournable qu'est la cyberassurance, et peut-être même la cryptomonnaie, puisque ces deux phénomènes sont également assez récents dans le paysage. Qu'en pensez-vous, Stephen?

Stephen Burns (25:18): Pour ce qui est de l'assurance, les compagnies d'assurance cherchent avant tout à bien évaluer les risques qu'elles couvrent afin de facturer des primes adaptées et proportionnées au niveau de risque assumé.

Dans le secteur de la cyberassurance, qui évolue très rapidement, on observe de plus en plus d'exclusions, un renforcement des vérifications, ainsi qu'une évaluation plus approfondie de la manière dont une organisation protège ses données et ses systèmes. Cela permet de mieux adapter les garanties proposées et les primes demandées au risque réel auquel l'organisation est exposée.

Autrefois proposée comme une couverture complémentaire, la cyberassurance prend désormais la forme d'une police à part entière, bien plus encadrée et réfléchie. C'est d'ailleurs un excellent réflexe pour les conseils d'administration de se poser la question que vous venez de me poser, soit : « Où en sommes-nous avec notre cyberassurance, et sommes-nous bien couverts? » Cette assurance fournit une perspective externe sur la situation de l'organisation et la manière dont elle gère ses risques, et cela se traduit directement par le montant des primes exigées.

Rahul Bhardwaj (26:28): En ce qui concerne la cryptomonnaie, ce thème semble omniprésent, puisqu'à mon avis, il recouvre bien des aspects abordés ici, et revient régulièrement dans différentes conversations.

Stephen Burns (26:35): Effectivement, et c'est surtout vrai dans le domaine des cyberrisques. La chaîne de blocs est un outil très utile qui, lorsqu'il est correctement utilisé, peut optimiser la manière dont les organisations mettent leurs produits et services sur le marché.

Au-delà de l'utilisation de la chaîne de blocs comme un outil, il y a l'idée de l'utiliser comme une cryptomonnaie ou comme un instrument de valeur. Puisqu'elle ne passe pas par le système bancaire, elle constitue un moyen de paiement privilégié pour les auteurs de menace.

On parle beaucoup de la situation où, en cas d'attaque par rançongiciel, il faudrait probablement payer la rançon en cryptomonnaie. Comment assurer le financement de cette somme? Faut-il conserver une réserve de cryptomonnaie?

La question de savoir s'il faut ou non conserver une certaine quantité de cryptomonnaie relève plutôt de l'équipe de la trésorerie ou du contrôleur de gestion, qui devront déterminer la bonne répartition des actifs à avoir dans ce domaine.

Cela dit, il me semble plus pertinent de ne pas se concentrer uniquement sur la manière de payer en cas d'attaque, mais plutôt de s'assurer que des mesures adéquates sont prises pour protéger les actifs les plus précieux. Il est également essentiel de bien comprendre l'ordre d'importance des données et des systèmes opérationnels.

Rahul Bhardwaj (28:00): Bon, Stephen, nous avons commencé cette conversation en soulignant que l'IA existe depuis longtemps sous diverses formes, et que les conseils d'administration ont su s'adapter pour gérer à la fois les risques et les opportunités qu'elle présente. Et nous voilà maintenant à parler de cyberassurance avancée et de cryptomonnaie, des sujets qui ne faisaient pas partie du paysage initial de l'IA, ni du vocabulaire des administrateurs, et encore moins de leurs processus.

Cela nous amène maintenant à la résolution sur laquelle je vais vous demander de vous prononcer : « Il est résolu que les conseils d'administration doivent repenser fondamentalement les cyberrisques à l'ère de l'IA. »

Stephen Burns (28:39): Je suis d'accord avec cette résolution, surtout après notre discussion. Toutefois, il y a beaucoup de changements en cours. Il y a beaucoup de nouvelles fonctionnalités et de nouvelles capacités, et ce n'est que le début. D'importantes sommes sont investies dans la recherche. Plusieurs défis ont déjà été relevés. L'IA ou les outils de l'IA sont désormais capables de faire des choses incroyables, et ce n'est pas près de s'arrêter.

Ces outils ne sont que des outils. Ils agissent sur les données et les opérations. Pour chaque auteur de menace qui parvient à s'en servir pour devenir plus efficace, nous devons, nous aussi, nous améliorer dans ce que nous faisons. Cela demande une vraie mobilisation de notre part. C'est pourquoi je soutiens pleinement l'idée de repenser notre manière d'aborder les cyberrisques.

Rahul Bhardwaj (29:24): Comme vous l'avez mentionné, il y a encore beaucoup à venir. Cela signifie, Stephen, que vous et moi allons nous retrouver à nouveau pour en discuter quand la situation aura un peu évolué. Merci de vous être joint à nous aujourd'hui. Je trouve que cet échange a été particulièrement intéressant et très diversifié.

À notre public, j'espère que vous avez aimé l'épisode Be It Resolved d'aujourd'hui, que vous avez pu approfondir vos connaissances en ce qui a trait aux salles du conseil et que cela vous aidera à rester au fait de ces nouvelles tendances. Si vous avez apprécié l'épisode, veuillez vous abonner, évaluer l'épisode et laisser un commentaire sur votre plateforme de diffusion en continu préférée. C'était Rahul Bhardwaj, de l'Institut des administrateurs de sociétés du Canada. À la prochaine fois.