POINTS DE VUE
D'AUDIT INTERNE

CYBERSÉCURITÉ ET CONFIANCE NUMÉRIQUE

IAI
Canada
Montréal

Introduction

La cybersécurité est devenue une préoccupation majeure pour les entreprises de toutes tailles et de tous secteurs. Les cyberattaques peuvent causer des pertes importantes en termes financiers et de réputation, en compromettant la confidentialité, l'intégrité et la disponibilité des données.

Dans ce contexte, la fonction d'audit interne peut jouer un rôle clé pour aider les entreprises à se protéger contre les risques liés à la cybersécurité. Pour en savoir plus sur ce sujet, nous avons interviewé Alexandre Bercovy qui a travaillé pendant plusieurs années en audit interne avant de prendre la responsabilité de la gestion intégrée des risques dans son entreprise actuelle. Dans cette entrevue, nous avons discuté des éléments clés de la cybersécurité et de la confiance numérique, du rôle de l'audit interne dans la cybersécurité, et des défis et opportunités dans ce domaine critique.

BIOGRAPHIE

Biographie

Alexandre Bercovy est un expert en gestion intégrée des risques. Son parcours de 30 ans en services professionnels et postes opérationnels est axé sur l'analyse des risques technologiques. Il a servi de nombreux clients dans les industries bancaires, transport, pharmaceutique et services en menant des mandats d'audit et de conseil complexes et multinationaux.

Son expérience englobe la prise en compte des enjeux technologiques dans le domaine de la cybersécurité, la mise en place du modèle des 3 lignes de défense, l'identification et l'évaluation des risques, des contrôles et objectifs associés, la gestion de programmes et de projets, et la conduite du changement.

Il est actuellement directeur de la gestion intégrée des risques chez Investissement Québec. Il est également président ex-officio du chapitre Montréalais de l'ISACA et détient les titres d'auditeur certifié des SI (CISA), CGEIT (certifié en gouvernance des TI), CRISC (Certifié en gestion des risques technologiques) et CDPSE (Protection des données personnelles).

Entrevue

01 Avant de plonger dans le vif du sujet, j'aimerai débuter en définissant les termes clés et mieux comprendre les différences conceptuelles entre les technologies de l'information, la cybersécurité et la confiance numérique ou le « digital trust » en anglais?

Les technologies de l'information (TI) font référence à l'ensemble des outils, des systèmes et des infrastructures utilisés pour collecter, stocker, gérer et échanger des informations. Cela englobe les actifs hardware : ordinateurs, serveurs, routeurs, disques, baies, réseaux, et software, logiciels, les bases de données, etc. qui fournissent des capacités de calcul, de stockage, de transport et de sécurisation des données. Les TI sont essentielles pour le fonctionnement des organisations, car elles permettent la gestion des données, l'automatisation des processus et la communication. De nos jours la dépendance envers les TI est devenue critique.

La cybersécurité, quant à elle, se concentre sur la protection de ces technologies de l'information contre les menaces et les attaques malveillantes. Elle vise à prévenir les accès non autorisés, les perturbations, les vols de données et les dommages causés aux systèmes informatiques. La cybersécurité implique des mesures techniques, organisationnelles et humaines pour garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes.

Enfin, la confiance numérique est une notion plus large et plus humaine. Elle concerne la confiance que nous accordons aux outils et aux technologies numériques qui sont omniprésents dans notre vie quotidienne, que ce soit sur le plan professionnel ou personnel. La confiance numérique pose des questions telles que : pouvons-nous avoir confiance dans la sécurité de nos transactions en ligne ? Pouvons-nous faire confiance aux opérateurs auxquels nous confions nos données personnelles, que ce soit pour nos interactions sociales ou pour les stocker dans le cloud ? Comment pouvons-nous être sûrs que nos interactions en ligne sont authentiques et légitimes?

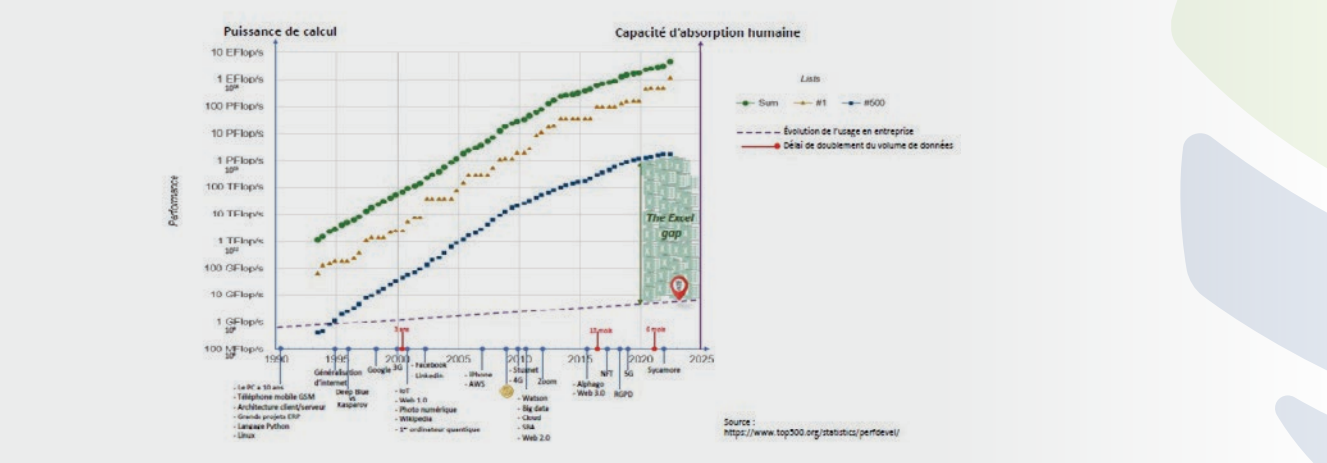
La confiance numérique englobe la sécurité des technologies de l'information et va au-delà en incluant des aspects éthiques. Par exemple, nos données peuvent être très bien protégées par un opérateur qui va néanmoins les revendre à ses partenaires commerciaux. Il s'agit de garantir que nos actions quotidiennes en ligne sont protégées et que nous pouvons avoir confiance dans les services numériques que nous utilisons en ayant une visibilité effective sur la façon dont nos données personnelles vont être traitées.

En résumé, les technologies de l'information sont les outils et les systèmes utilisés pour gérer les informations, la cybersécurité se concentre sur la protection de ces technologies contre les menaces, tandis que la confiance numérique englobe la confiance que nous accordons aux outils et aux interactions numériques dans leur ensemble.

02 Quels sont actuellement les défis les plus importants auxquels les entreprises sont confrontées en matière de cybersécurité?

La cybersécurité est une préoccupation permanente, car les cyber-attaques sont devenues plus fréquentes (pour ne pas dire quotidiennes), plus sophistiquées et plus diversifiées. Il est essentiel de reconnaître que la question n'est pas de savoir si un objet ou un système sera piraté, mais plutôt quand, par qui, combien de fois et comment cela se produira.

Le graphique ci-dessous, développé sur base de données publiques, explique l'écart entre l'évolution technologique et la capacité d'absorption humaine. Il met en lumière les jalons temporels clés de la cybersécurité et il en découle plusieurs grands défis liés à la cybersécurité.



Parmi les grands défis, il y a tout d'abord les cyberattaques ciblées. Les entreprises sont constamment la cible d'attaques visant à voler des données sensibles, à perturber les opérations ou à compromettre leur réputation. Ces attaques peuvent provenir de groupes de cybercriminels, d'États-nations ou d'agents internes (employés) malveillants.

Il y a aussi la vulnérabilité des infrastructures critiques, telles que les réseaux électriques, les systèmes et matériels de transport ou les services de santé, qui sont de plus en plus connectées et dépendantes des technologies de l'information. Des attaques à ce niveau-là peuvent entraîner des conséquences dévastatrices sur la société. On peut prendre les exemples de l'attaque subie par la STM en novembre 2020, le Colonial Pipeline aux États-Unis en 2021 ou encore les avions d'Air Canada perturbés par de faux signaux GPS en mars 2024.

L'émergence de nouvelles technologies telles que l'Internet des objets (IoT), l'intelligence artificielle (IA) et la blockchain a créé de nouvelles opportunités, mais aussi de nouveaux défis en matière de cybersécurité. Ces technologies introduisent de nouveaux vecteurs d'attaque et nécessitent des mesures de sécurité adaptées.

De plus, les entreprises doivent se conformer à un ensemble croissant de réglementations en matière de protection des données et de confidentialité, telles que le Règlement général sur la protection des données (RGPD) en Europe ou la Loi 25 au Québec. Le non-respect de ces réglementations peut entraîner des sanctions financières importantes.

Finalement, je pense aux employés qui sont souvent considérés comme le maillon faible de la sécurité informatique. Les entreprises doivent investir dans la sensibilisation et la formation de leur personnel pour les aider à reconnaître les menaces et à adopter de bonnes pratiques en matière de sécurité. Par exemple, l'utilisation d'Excel est omniprésente. Cependant, il est important de noter que l'utilisation d'Excel ne garantit pas une sécurité accrue pour les données stockées. Plus précisément, les utilisateurs ne sont pas suffisamment conscients des risques liés au partage de fichiers Excel contenant des données sensibles voire confidentielles. Je ne crois pas que l'humain comme maillon faible soit une fatalité, mais l'effort de sensibilisation est un travail de chaque instant.

03 Quels sont les rôles clés dans une organisation en matière de cybersécurité?

Les opérations, dont font partie les TI, et les lignes d'affaires sont responsables de la mise en œuvre des contrôles de sécurité et de la gestion des risques au niveau opérationnel. Ils sont les premiers acteurs à être confrontés aux menaces et doivent donc être conscients des risques et des bonnes pratiques de sécurité. Cela inclut par exemple la protection de l'infrastructure, la sensibilisation et la formation des employés, la mise en place de politiques de sécurité, une gestion efficace des accès et des autorisations, ainsi que la surveillance des activités pour détecter les incidents de sécurité.

Le travail de concert avec les lignes d'affaires est clé. Par exemple, la gestion des identités et des accès n'est pas, ou peu, un sujet technique. Ce ne sont pas les TI qui décident qui a accès à quoi, mais bien les opérationnels, donc la première ligne. La mise en œuvre de ces règles relève quant à elle des TI. Dans ce contexte, la 2ème ligne peut – et doit – jouer son rôle d'identification, d'évaluation, d'analyse des risques de cybersécurité, pour la fournir aux équipes TI en même temps que sa perspective. Elle doit aussi tester les mesures de mitigation et proposer des plans d'actions lorsque nécessaire. Cela est donc très proche de la démarche d'audit cependant avec un positionnement différent.

Les fonctions de gouvernance, de gestion des risques et de conformité jouent un rôle crucial dans la supervision et la coordination de la cybersécurité. Ces fonctions d'assurance établissent les politiques et les procédures de sécurité, effectuent des évaluations des risques, les tests, surveillent la conformité aux réglementations et aux normes de sécurité, et fournissent des conseils et des orientations aux opérations pour renforcer la posture de sécurité de l'organisation. Elles assurent également une coordination avec les parties prenantes internes et externes, y compris les organismes de réglementation et les partenaires commerciaux.

Les fonctions d'audit interne et de gestion des risques sont responsables de l'évaluation indépendante de l'efficacité des contrôles de sécurité et de la gouvernance de la cybersécurité. La gestion des risques produit les encadrements (politiques, directives, procédures) et recense les mesures de mitigation (contrôles de sécurité). L'audit interne et gestion des risques fournissent des recommandations pour améliorer la posture de sécurité de l'organisation. Ils jouent également un rôle de conseil et de vérification pour s'assurer que les mesures de sécurité sont adéquatement conçues et opérées efficacement.

Un facteur clé de succès est que tout ce monde travaille de concert. Pour rester pertinent au regard de la cybersécurité, la formation et la gestion du changement doivent être des éléments fondamentaux et chaque acteur a un rôle à jouer dans la promotion d'une culture de sécurité au sein de l'organisation et dans la sensibilisation des employés aux risques et aux bonnes pratiques de sécurité. Concrètement, il me paraît essentiel que les fonctions de gouvernance, de gestion des risques et de conformité portent ce message auprès des opérationnels en parlant leur langage.

04 Spécifiquement pour les fonctions d'audit interne, comment peuvent-elles se préparer pour faire face aux défis de la cybersécurité ?

Les normes ont été mises à jour récemment. Je paraphrase mais l'audit est maintenant défini comme un vecteur de valeur pour l'entreprise pour qu'elle atteigne ses objectifs. Elle fait le lien entre les opérations et le comité d'audit à qui elle rend des comptes. C'est un outil puissant qui a toute sa légitimité pour participer à des enjeux de taille tel que la cybersécurité et qui de surcroît a une position de choix au sein de l'entreprise.

À mon sens, l'audit interne a plusieurs défis devant elle.

Tout d'abord, elle doit se doter de professionnels compétents en matière de cybersécurité. Cela peut impliquer le recrutement de spécialistes de la cybersécurité ou la formation continue des auditeurs internes existants pour développer leurs compétences dans ce domaine. Dans un marché tendu, cela n'est pas toujours simple.

Une fois dotée de personnels compétents, l'audit interne doit être en mesure de comprendre et de documenter les requis complexes de cybersécurité afin de pouvoir les évaluer correctement. On peut prendre l'exemple du domaine RA (Risk Assessment) du NIST 800-53. Cela peut nécessiter une collaboration étroite avec les équipes de cybersécurité et l'accès à des informations détaillées sur les contrôles et les mesures de sécurité requises ou mises en place. Seule une documentation claire et complète peut permettre à l'audit interne de réaliser des tests efficaces et de formuler des recommandations pertinentes.

Je pense aussi à l'accès aux données en temps opportun. L'audit interne peut rencontrer des obstacles lorsqu'il s'agit d'obtenir l'accès aux données nécessaires pour évaluer la cybersécurité. Le comble, c'est que parfois cela peut être dû à des règles de sécurité. Pourtant, ce n'est qu'en faisant parler les données que l'audit peut produire des résultats précis. Il est donc important que la charte de l'audit interne prévoie cet accès sans restriction, et qu'il soit appliqué dans les faits.

De plus, il est important de travailler en étroite collaboration avec les opérations pour comprendre leurs préoccupations en matière de sécurité et trouver des solutions qui répondent à la fois aux recommandations de l'audit sans faire suffoquer les secteurs d'affaires. Trop de contrôle tue le contrôle. L'arbitrage coûts/bénéfice doit être omniprésent dans les discussions et les décisions. Cela peut inclure des discussions sur les mesures de protection des données et la mise en place de protocoles pour faciliter l'accès aux données pertinentes de manière sécurisée.

Finalement, l'audit interne doit adopter une vision holistique et globale de la cybersécurité plutôt que de se limiter à des aspects spécifiques. Comprendre les enjeux et les tendances actuelles en matière de cybersécurité est essentiel pour évaluer les risques, les mettre en perspective et conseiller sur les mesures à prendre pour renforcer la posture de sécurité de l'organisation. Prenons l'exemple concret du coût moyen d'une violation de données, qui est estimé à 4+ millions de dollars US et qui continue d'augmenter. Il est également important de noter que les compagnies d'assurance cyber sont de plus en plus réticentes à assurer les entreprises. Ces tendances soulignent le besoin pour les organisations de renforcer leur posture de sécurité et de mettre en place des mesures de prévention et de protection efficaces. Il ne faut pas être resigné ou désabusé mais il faut être réaliste. Jusqu'à la pandémie, les attaques par rançongiciel étaient vécues comme une affaire d'argent. Elles sont aujourd'hui un enjeu de continuité d'activité, et cela change beaucoup de choses.

Face à l'évolution constante des risques de cybersécurité, il faut être prêt à agir rapidement et efficacement en cas d'incident. On ne peut pas avoir d'opinion tranchées et nous sommes bien incapables d'imaginer les risques futurs et leur ampleur. Il faut être agile et savoir quoi faire pour assurer la continuité d'affaire. Il faut avoir des bons réflexes et cela nécessite de l'entraînement. Pour tout cela, l'audit interne doit être prête à se positionner en rôle conseil.

05 J'aimerais revenir au concept de confiance numérique. Pour m'assurer de bien comprendre, pourrais-tu me donner un exemple concret?

On pourrait prendre l'exemple de la tarification dynamique utilisée par certaines plateformes de covoiturage ou de réservation de taxis pour bien comprendre le facteur de confiance au-delà des aspects techniques

Lors d'un événement exceptionnel, comme les attentats de Londres en 2017, la gestion de crise a entraîné une forte demande de déplacements hors des zones dangereuses. Dans cette situation, les taxis traditionnels ont réagi en offrant des trajets gratuits pour aider les personnes à se mettre en sécurité. Cependant, l'algorithme d'Uber, qui fonctionne sur la base de la tarification dynamique, a augmenté les prix en raison de la forte demande. L'algorithme a détecté une augmentation de la demande et a ajusté les prix en conséquence, conformément à sa programmation. Cela a suscité un scandale, car les utilisateurs ont perçu cela comme une exploitation de la situation d'urgence et ont remis en question la confiance envers Uber.

Cet exemple met en évidence l'importance de l'éthique dans la confiance numérique. Les utilisateurs s'attendent à ce que les entreprises prennent en compte les valeurs éthiques tant au quotidien que lors de situations exceptionnelles.

Un autre exemple courant de confiance numérique concerne l'utilisation d'un VPN. Les utilisateurs font confiance à un fournisseur de VPN pour protéger leur confidentialité en sécurisant leurs données et en masquant leur adresse IP. Cependant, il existe des préoccupations quant à savoir si le fournisseur de VPN peut lui-même revendre les données des utilisateurs à des tiers. Cela va à l'encontre même du service demandé. Pourtant c'est une pratique répandue, en particulier chez les opérateurs qui fournissent un service gratuit.

Pour simplifier, la confiance numérique se manifeste dans des situations où les utilisateurs doivent faire confiance aux algorithmes, aux plateformes et aux pratiques des fournisseurs de services numériques pour protéger leurs données et agir de manière éthique. La loi impose désormais le consentement libre et éclairé pour les utilisateurs, mais dans les faits, il y a encore des progrès à faire.

06 Quel est l'avenir des risques et des contrôles si l'on y pense en termes de confiance numérique?

C'est très complexe et en constante évolution. La conformité réglementaire est un point d'ancrage important pour créer un cadre éthique, mais elle est souvent en retard par rapport aux risques émergents. Et quand bien même, la nature humaine est en permanence en train d'arbitrer entre le coût de la conformité et celui de la sanction pour non-conformité. C'est la base de la gestion de risques. Cependant, le respect d'un cadre éthique va au-delà de cet arbitrage car il définit les valeurs réelles de l'entreprise. Une étude récente a démontré que les entreprises qui construisent et respectent un cadre éthique sont mieux valorisées que celles qui n'en ont pas.

Un défi majeur pour l'avenir des contrôles est la vélocité du changement. Les avancées technologiques, notamment l'intelligence artificielle, créent de nouveaux risques. Par exemple, les « hypertrucages », qui étaient initialement utilisés pour des vidéos humoristiques, sont maintenant utilisés dans des activités frauduleuses, y compris la fraude vocale pour l'identification. On a vu un exemple spectaculaire de fraude utilisant des « deepfakes » pendant une réunion Teams à Hong Kong en février 2024 (coût de 25M$ US). Cette évolution rapide et imprévisible des technologies rend difficile la prédiction de ce à quoi l'avenir ressemblera en matière de risques et de contrôles.

Ce que nous pouvons faire est de rester à jour avec les nouvelles technologies, les tendances en matière de cybersécurité et les meilleures pratiques de contrôle. C'est une période incertaine et stimulante.

Les auditeurs internes font face à de grands défis pour accompagner les organisations face aux enjeux de la cybersécurité et de la confiance numérique. Ces défis s'accompagnent également de belles opportunités pour faire progresser la profession et apporter de la valeur aux organisations.

07 Justement, as-tu des sources d'information à recommander pour des auditeurs internes qui souhaiteraient approfondir ce dont nous avons parlé?

L'Institut des Auditeurs Internes (IIA) propose un large éventail de ressources pour approfondir les concepts de cybersécurité. Je recommande particulièrement leur nouveau GTAG intitulé « Auditer les opérations de cybersécurité : prévention et détection », qui aide les auditeurs à mieux comprendre les objectifs de contrôle en cybersécurité. Ce guide est essentiel pour renforcer la valeur ajoutée des missions d'audit et de conseil, et inclut des ressources complémentaires pour approfondir ces sujets.

L'IAI Montréal propose également diverses formations, telles que :

- Audit de la cybersécurité
- Nouveau ! Des tests de conformité financière aux CGTI : comment bien négocier le virage?
- Rapports SOC : les démystifier pour mieux en tirer partie

L'ISACA propose également des ressources précieuses en matière de gouvernance, de risque et de conformité liés à la cybersécurité.

De plus, voici d'autres ressources pertinentes :

- Étude sur le cadre éthique : Cet article explore si l'éthique est rentable pour les entreprises. Lire l'étude.
- Article sur le Digital Service Act (DSA) : Le DSA est entré en vigueur dans l'Union européenne et vise à réglementer les grandes plateformes numériques. En savoir plus.
- Éthique dans la gestion des données : Cet article de Dominique Rouziès et Michael Segalla, publié dans la Harvard Business Review, explore les défis éthiques liés à la gestion des données personnelles. Lire l'article

Entrevue réalisée par
Maelle Gillet pour l'Institut des auditeurs internes – Section Montréal

À propos de l'ISACA

L'ISACA est une association internationale qui regroupe plus de 150 000 membres dans 188 pays, et rassemble aujourd'hui plus d'un millier de professionnels à Montréal. Sa vocation est d'aider les organisations à mettre le système d'information au service de leur stratégie et de leur gestion du risque technologique. Notre chapitre veille notamment à former les professionnels, en les préparant aux certifications professionnelles internationales délivrées par l'ISACA autour de la gouvernance et de la maîtrise des SI : CISA, CRISC, COBIT, ITAF, Val IT, Risk IT, BMIS, mais aussi à la gouvernance, au management des SI et à la gestion des risques cyber.

À propos de l'IAIM

Fondé en mars 1945, l'Institut des auditeurs internes, Section Montréal (IAI Montréal) est un organisme à but non lucratif constitué en vertu de la loi sur les compagnies du Québec. Il regroupe près de 900 membres et est dirigé par un conseil d'administration, supporté par des comités.

Notre chapitre a pour mission de soutenir et développer les professionnels de l'audit interne tout au long de leur carrière, ainsi que de promouvoir le rôle et la valeur de la profession. Sa vision est d'être reconnu comme un partenaire de choix par la communauté d'affaires, qui veille à la pertinence et l'innovation au sein de la profession.

Notre slogan? Le partenaire par excellence pour la croissance de nos membres!

IAI
Canada
Montréal