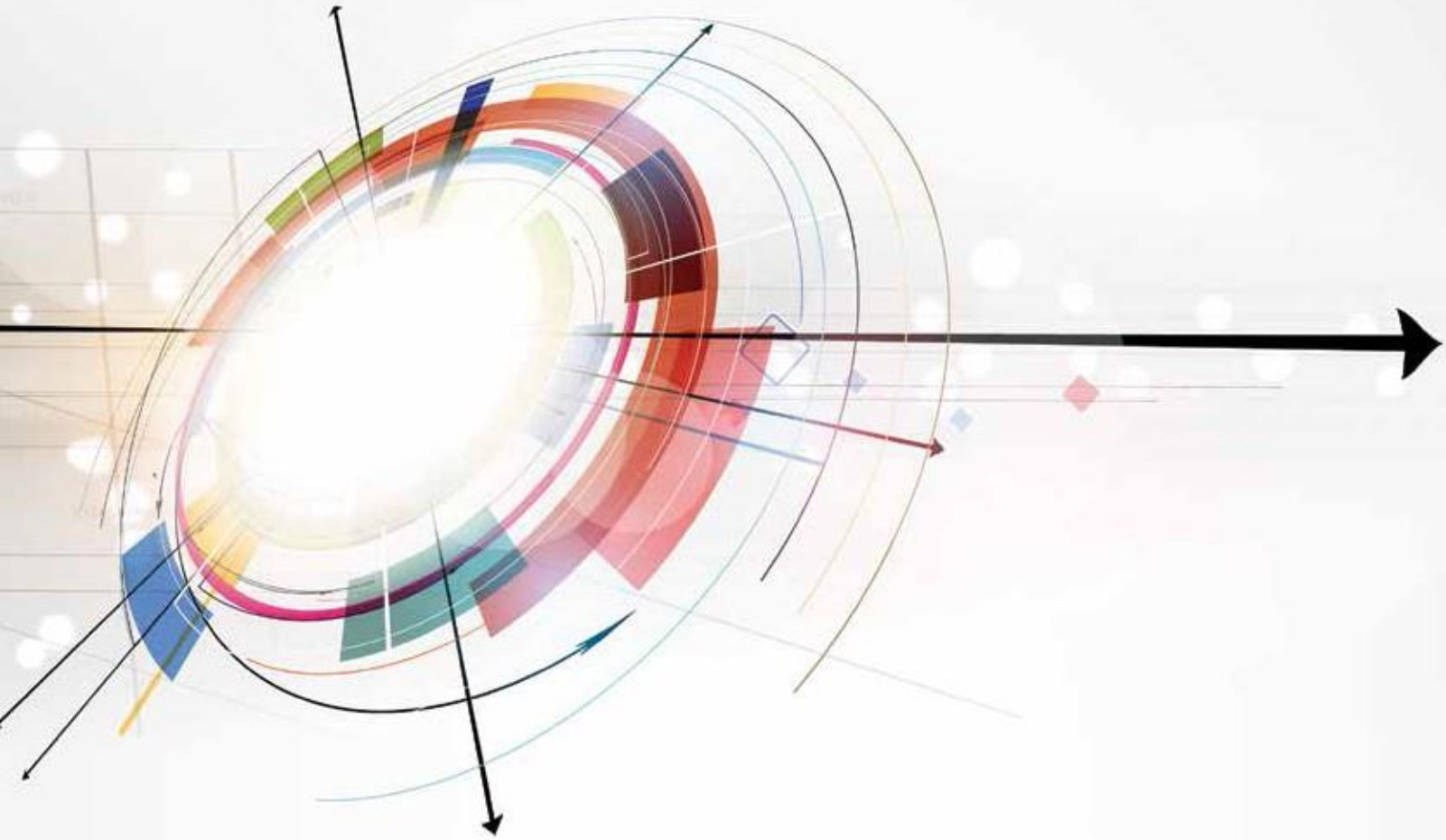

Numéro 4

PERSPECTIVES INTERNATIONALES

L'audit interne, conseiller digne de confiance en cybersécurité

The Institute of Internal Auditors | Global

Table des matières

Contributeurs

Municipalité de Cape Town – *Afrique du Sud*
Lindiwe Ndaba, CIA, Responsable de l'audit interne
Etienne Postings, CIA, CCSA, CISA, Directeur de mission : audit des systèmes d'information
Andre Stelzner, Directeur, systèmes d'information et technologies

FirstRand Ltd – *Afrique du Sud*
Jenitha John, CIA, QIAL, CA(SA), Responsable de l'audit interne

Insurance Australia Group Limited – *Australie*
Jeff Jacobs, Responsable de la sécurité des systèmes d'information
Lee Sullivan, Responsable de l'audit interne

RSM US LLP – *États-Unis*
Daimon Geopfert, Responsable national des services de sécurité et de confidentialité des données

Saudi Basic Industries Corporation (SABIC) – *Arabie saoudite*
Gregory Grocholski, CISA, vice-président, Responsable de l'audit interne

Institute of Internal Auditors – *États-Unis*
Greg Jaynes, CIA, CRMA, CFE, CGFM, Responsable de l'audit interne
Charles Redding, vice-président exécutif et directeur des systèmes d'information

Universidad de Los Andes – *Colombie*
Jeimy Cano, CFE, certification Cobit5 Foundation
professeur émérite, Faculté de droit

Université de Virginie – *États-Unis*
Jason Belford, Directeur des systèmes d'information
Gerald Cannon, CISA, CRISC, Responsable De l'audit des systèmes d'information
Virginia Evans, Directrice des systèmes d'information
Ron Hutchins, vice-préidente de IT
Carolyn Saint, CIA, CRMA, CPA, Responsable de l'audit interne

Commentaires

N'hésitez pas à nous faire parvenir vos questions et vos commentaires à l'adresse suivante : **globalperspectives@theiia.org**.

L'auditeur interne, conseiller digne de confiance en cybersécurité

S'il est impossible de *tout* savoir sur un sujet aussi complexe et évolutif, il est devenu essentiel pour un responsable de l'audit interne de s'y connaître en cybersécurité. En fait, étant donné la nature dynamique des risques encourus, un responsable de l'audit interne bien informé peut positionner l'audit interne comme un conseiller digne de confiance de l'organisation sur ce sujet épineux et très médiatisé.

Les statistiques sont alarmantes :

> En 2015, le coût moyen d'une violation de données était de 3,79 millions de dollars. Un impact en hausse par rapport aux 3,52 millions estimés en 2014 et 23 % plus élevé qu'en 2013.
> Ce coût tient compte d'effets tels que la rotation anormale de la clientèle, la multiplication des actions pour attirer les clients, les atteintes à la réputation et une dépréciation des écarts d'acquisition (*godwill)*.[1]
>
> Les cybercriminels avaient, en moyenne, pu accéder à l'environnement de l'organisation pendant 205 jours avant d'être découverts. Par ailleurs, 69 % des organisations étaient victimes d'attaques de tiers plutôt que de leurs collaborateurs.[2]
>
> Au cours du premier trimestre 2015, sur les 888 incidents mis à jour, près de 246 millions de fichiers ont été piratés. Par ailleurs, dans la moitié au moins de ces incidents, le nombre exact de fichiers piratés n'a pas pu être déterminé.[3]
>
> Les cyberattaques sont un phénomène mondial. Au cours du premier semestre 2015, l'Amérique du Nord a été la principale cible de ces attaques (707 incidents), suivie du Royaume-Uni (94) et de l'Asie (63). Cinq des dix attaques les plus importantes, en nombre de fichiers de données corrompus, concernaient des organisations non basées aux États-Unis.

Au vu des statistiques, il n'est pas étonnant que Amit Yoran, président de RSA, s'exclame : « *Le secteur de la [cyber] sécurité échoue. Il a échoué.* »[5]

[1] IBM et Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis*, à partir d'une étude menée auprès de 350 organisations dans 11 pays.

[2] Mandiant, *M-Trends 2015: A View from the Front Lines*, étude compilant les résultats des enquêtes sur les réponses aux menaces menée dans plus de 30 secteurs.

[3] Gemalto, indice BLI (Breach Level Index), base de données recensant toutes les violations de données rendues publiques à travers le monde.

[4] *Ibid.*

[5] Hackett, R.;*Security Has Failed: Exclusive Preview of RSA President's Conference Preview Fortune*, 21 avril 2015.

Pourtant, personne ne songe à mettre en cause l'importance de la cybersécurité, autrement dit des mesures prises pour protéger les données des systèmes connectés à Internet contre les risques de perte, de destruction, d'accès non autorisé ou d'utilisation abusive. De nombreuses personnes brillantes et réfléchies se penchent sur la question depuis des années. Leurs prévisions sont réalistes ; en effet, rares sont ceux qui pensent que les cyberattaques peuvent être entièrement éliminées. Comme le note Jeimy Cano, professeur émérite à la faculté de droit de l'Universidad de los Andes, dans l'environnement numérique d'aujourd'hui, l'incident est devenu une fatalité. L'enjeu de la cybersécurité consiste à minimiser les dégâts. L'objectif est de bloquer autant d'attaques que possible et, dans le cas, inévitable, d'une intrusion, de trouver les criminels avant qu'ils n'aient accès aux informations les plus sensibles.

Un travail d'équipe

Cette tâche n'est pas réservée aux experts en cybersécurité. La question doit être envisagée de façon globale et systématique, les conséquences d'un incident pouvant aller de la simple incapacité à conclure des transactions élémentaires jusqu'à la perte de propriété intellectuelle et à l'atteinte à la réputation. Le risque n'est pas seulement technologique ; il est également opérationnel. C'est pourquoi les auditeurs internes ont un rôle essentiel à y jouer. Leur succès dépend fortement de la priorité que le Conseil ou le comité d'audit donne à cette question et de l'approche du responsable de l'audit interne. La cybersécurité offre à ce dernier l'occasion de se positionner comme un conseiller digne de confiance, en proposant à l'organisation des orientations avisées, fondées sur la stratégie et l'anticipation, plutôt que de simplement s'assurer que les missions dans ce domaine sont exécutées conformément au plan d'audit. Cela implique d'évaluer les cyberisques et leur impact sur la stratégie et la réputation de l'organisation ; de favoriser, en temps utile, des discussions ciblées entre le management et les dirigeants ; et d'insister sur la nécessité de faire preuve de vigilance et de se doter de ressources suffisantes en la matière.

Le responsable de l'audit interne est également bien placé pour établir de fructueuses et étroites relations de collaboration avec le directeur des systèmes d'information et le directeur de la sécurité des systèmes d'information. De telles relations peuvent améliorer la compréhension parfois approximative des attentes et des besoins des équipes chargées de la sécurité et des systèmes d'information, ou de ce que l'audit interne peut leur apporter. Selon Jenitha John, responsable de l'audit interne chez FirstRand Ltd, les responsables de la sécurité des systèmes d'information souhaitent obtenir de l'audit interne un point de vue honnête et proactif sur les tendances actuelles et les questions présentes et émergentes qui prédominent dans leur environnement — autrement dit la vision prospective et proactive d'un conseiller digne de confiance. Jenitha John estime que l'audit interne doit « envisager ces questions au regard des risques encourus et des conséquences que ceux-ci sont susceptibles d'avoir sur l'organisation. »

Charles Redding, vice-président exécutif et DSI de l'IIA, estime que les directeurs des systèmes d'information ont des besoins similaires, quoique distincts, de ceux de leurs homologues en charge de la sécurité des SI. Il précise que ces derniers ont tendance à aborder la question de la cybersécurité sous l'angle technique. L'audit interne élargit cette perspective en fournissant à la direction générale les informations qui les « *aideront à évaluer le risque et à définir les seuils de tolérance au risque*. » La fonction d'audit interne à laquelle il fait allusion est celle dirigée par Greg Jaynes qui témoigne du partenariat existant entre audit interne de l'IIA et le DSI : « *Lorsque Charles et moi-même sommes tous deux au bureau, il ne se passe pas un jour sans que nous ne parlions des risques et de la cybersécurité. Je ne vois pas comment un responsable de l'audit interne peut être efficace sans une étroite interaction avec le DSI.* »

Gregory Grocholski, vice-président et responsable de l'audit interne de Saudi Basic Industries Corporation (SABIC), confirme l'importance du travail d'équipe, mais souligne que le rôle du responsable de l'audit interne en matière de cybersécurité ne se limite pas à promouvoir des relations de partenariat au sein de l'organisation. Ce dernier doit comprendre que les données structurées (données au format prédéfini pour être traitées dans des applications métier ou des logiciels de gestion par exemple) coexistent avec les données non structurées (traitement de texte, supports multimédia etc.), et que ces deux types de données peuvent susciter l'intérêt de tiers non autorisés.

Le responsable de l'audit interne doit être familiarisé avec les différents canaux utilisés par les cybercriminels pour accéder aux données et les sortir de l'organisation. Il s'assure que ces canaux reçoivent l'attention qu'ils méritent au niveau approprié de l'organisation en fonction des besoins, des contrôles nécessaires, de l'impact des menaces et de la tolérance aux risques. Loin de pouvoir se contenter d'être prêts à réagir, les responsables de l'audit interne devraient, à chaque instant, faire preuve d'anticipation.

Le soutien des instances dirigeantes

Dans l'immense majorité des organisations, chaque grand projet nécessite l'agrément des instances dirigeantes. Pourtant, les Conseils se montrent réticents à soutenir sans réserve les efforts en matière de cybersécurité. Selon une étude récente, 26 % des personnes interrogées indiquent que le directeur de la sécurité des systèmes d'information ou le responsable de la sécurité présentent un état des lieux de la sécurité au Conseil seulement une fois par an ; un pourcentage à peu près équivalent d'entre eux (28 %) n'en font jamais. Près d'un tiers affirment qu'aucun membre ou comité du Conseil n'est associé à la gestion des cyberisques ; le comité d'audit n'intervient sur cette question que dans 15 % des cas seulement.[6]

[6] PwC, *US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey*, juillet 2015.

Toutefois, cette réticence traditionnelle semble s'atténuer. Les Conseils commencent à rechercher au sein de leur organisation plus d'informations sur la cybersécurité et les risques connexes. En effet, ils ont pris conscience de l'éventuel étendue des dégâts qu'une cyberattaque pouvait produire, mais ils doivent également tenir compte de la pression réglementaire. En juin 2014, Luis Aguilar, commissaire de la SEC (Securities and Exchange Commission) annonçait : « *La supervision, par le Conseil, de la gestion des cyberisques est essentielle pour s'assurer que les organisations prennent les mesures adéquates pour prévenir les dommages qui pourraient résulter de telles attaques et de s'y préparer... Les Conseils qui décident d'ignorer ou de minimiser l'importance de la surveillance en matière de cybersécurité le font à leurs propres périls*. »[7]

Les instances dirigeantes (Conseils, comités d'audit et direction générales) ont besoin d'informations pour assumer efficacement leurs responsabilités. L'audit interne, qui bénéficie d'un accès privilégié à ces différents interlocuteurs, peuvent contribuer à faire de la cybersécurité une de leurs priorités. Jenitha John estime que la mission du responsable de l'audit interne est claire : « *Les responsables de l'audit interne doivent introduire les recommandations de leurs missions au niveau de gouvernance approprié afin de bénéficier de l'attention requise et de pouvoir ensuite suivre et rendre compte des mesures correctives engagées*. » Lee Sullivan, responsable de l'audit interne d'Australia Group Limited (IAG) explique que son reporting offre au Conseil « *une vision indépendante de l'état réel de préparation d'IAG face aux cyberisques*. »

Afin d'être plus efficaces dans leur reporting dans ce domaine, les responsables de l'audit interne peuvent examiner avec attention les tendances du secteur, telles que l'évolution attendue de la réglementation, les nouvelles exigences en matière de couverture d'assurance et les actions collectives en justice récemment intentées, et prendre en compte ces tendances lors de la définition du périmètre des missions d'audit interne. Ils peuvent également envisager de donner une assurance quant à l'adéquation et à la mobilisation des ressources humaines (équipes chargées de la résolution des incidents ou tiers chargés de l'évaluation des risques, par exemple).

Les responsables de l'audit interne doivent également fournir des conseils sur les projets en cours, qu'il s'agisse de limiter les risques encourus, d'optimiser l'utilisation des ressources pour orienter les efforts vers les principaux risques, ou, si ces projets sont suffisamment robustes et rigoureux, de prévenir et détecter les menaces. Carolyn Saint, responsable de l'audit interne de l'Université de Virginie, note que l'audit interne, par son implication dans les projets de cybersécurité, peut venir renforcer les efforts du management, en donnant plus de poids au message adressé au plus haut niveau de l'organisation sur les moyens nécessaires.

[7] Security Intelligence, *Why is Your Board of Directors Finally Asking about Cyber Risks?*, 13 octobre 2015.

Questions connexes

Les défis inhérents à la cybersécurité ont mis en lumière la problématique de la cyber-résilience, à savoir les activités entreprises en amont, au cours, et en aval des incidents pour garantir la résilience des systèmes d'information et de communication (et ceux qui en dépendent) face aux attaques constantes des cyber-ressources. Il s'agit entre autres d'améliorer la connaissance et la sensibilisation de l'ensemble des collaborateurs en matière de cybersécurité afin de leur permettre de mieux appréhender la nature et l'impact des risques associés et de faire front uni face au risque de cyberattaque. Le responsable de l'audit interne peut montrer l'exemple en s'attachant à développer cette connaissance et cette sensibilisation au sein de son propre service. Selon l'édition 2016 du North American Pulse of Internal Audit de l'IIA, le manque d'expertise de l'équipe d'audit interne constitue le principal obstacle à leur prise en compte des cyberisques.[8]

Jason Belford, responsable de la sécurité des systèmes d'information de l'Université de Virginie, considère la cyber-résilience comme un principe essentiel en matière de cybersécurité, qui doit être géré séparément mais pas de manière totalement autonome. Ron Hutchins, DSI de l'université, partage ce point de vue : « *Nous cherchons à optimiser la disponibilité et la fiabilité des systèmes, mais nous sommes conscients que tous les services ne nécessitent pas le même niveau de protection*. »

Andre Stelzner, directeur des systèmes d'information et des technologies de la municipalité de Cape Town (Afrique du Sud), résume clairement le concept sous-jacent : « *Une organisation cyber-résiliente est une organisation qui est consciente de sa vulnérabilité.* » La sécurité et la résilience passent par une bonne connaissance des faiblesses et des actions mises en œuvre pour les maîtriser, ainsi que par la définition de plans de continuité pour pouvoir réagir et rebondir en cas de cyberattaque. Il s'agit clairement de la meilleure stratégie à adopter.

La protection des données et la préservation de leur confidentialité constituent deux autres éléments clés de la cybersécurité ; il s'agit de savoir comment sont manipulées et stockées les données, où elles sont stockées, qui est habilité à y accéder et comment. Insurance Australia Group Limited juge essentiel de préserver la confiance des clients, et le directeur du service client contribue également, aux côtés du responsable des données et du directeur de la sécurité des systèmes d'information, à la protection des données client. Dans de nombreuses organisations, la fonction chargée de la confidentialité des données contribue également à définir les normes pertinentes, et à élaborer les politiques et procédures. Elle a également bien souvent pour mission de sensibiliser les collaborateurs aux questions de cybersécurité.

[8] IIA, *2016 North American Pulse of Internal Audit*, février 2016.

L'audit interne devrait considérer ces responsables comme des parties prenantes essentielles, et la conformité à la législation dans ce domaine comme un élément clé de toutes les missions concernées. Sonder les fonctions chargées de la confidentialité des données et les auditer peut donner des indices supplémentaires quant à la robustesse de la cybersécurité au sein de l'organisation. Les propriétaires des données et des SI et l'équipe juridique/ chargée de la confidentialité des données devraient échanger et collaborer dans le cadre mis en œuvre par l'organisation dans ce domaine. Dans le cas contraire, cette défaillance mériterait des investigations complémentaires.

Conclusion

L'opinion des responsables de l'audit interne et des directeurs des systèmes d'information et de la sécurité des systèmes d'information est claire : la cybersécurité reste un enjeu incontournable. Nous traversons, selon Jeime Cano, « *une nouvelle révolution industrielle, et une nouvelle ère de transformation dominée par le numérique, les ruptures et la résilience*. » Les organisations désireuses de ne pas venir grossir les statistiques sur la violation des données doivent veiller à acquérir l'expertise adéquate ; financer leurs efforts de protection ; rester en phase avec les évolutions de la réglementation ; suivre les tendances mondiales en matière de cyber-attaques ; et impliquer l'ensemble des parties prenantes dans un combat sans relâche contre les risques de perte ou d'atteinte à l'intégrité des données. Il n'en faut pas moins pour réussir.

Le responsable de l'audit interne qui remplit sa mission de conseiller digne de confiance a un rôle important à jouer en la matière. Pour assumer ce rôle, il doit maîtriser les enjeux de cybersécurité et le faire savoir, développer la confiance, et faire preuve de diplomatie et de sensibilité pour poser les bonnes questions au bon moment et aux bonnes personnes. L'organisation fait-elle preuve d'une approche cohérente en matière de cybersécurité ? Les politiques et procédures adoptées soutiennent-elles cette philosophie ? Que font les autres organisations et comment se situer par rapport à ces dernières ? Ces interrogations doivent s'accompagner d'une écoute active et attentive, et la recherche de réponses doit passer par la mise en œuvre de l'expertise métier, de la connaissance de l'organisation et de son environnement et des connaissances liées aux technologies.

Pour réussir en matière de cybersécurité, il faut être conscient qu'il existe des individus à l'intérieur et à l'extérieur de l'organisation qui ne reculeront devant rien pour accéder aux données de cette dernière. Parce qu'ils ne relâcheront pas leurs efforts, l'organisation visée ne doit pas relâcher les siens. Les paroles de Grocholski résument bien la situation actuelle : « *Nous vivons à l'ère du numérique. Il est impératif de protéger ses actifs dans ce domaine comme on protège sa maison et sa famille*. »

Pour plus d'informations

International Organization for Standardization, *ISO/IEC 27001 – Information security management*, 2013 (*www.iso.org*)

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, février 2014 (*www.nist.gov*)

Privacy by Design, (*www.ipc.on.ca/english/Privacy/Introduction-to-PbD*)

The IIA, *Cybersecurity:* Keeping IP Under Lock and Key, *Tone at the Top*, février 2014 (*www.globaliia.org/Tone-at-the-Top*)

The IIA, *The Cybersecurity Imperative*, Internal Auditor, Août 2015 (*https://iaonline.theiia.org*)

The IIA, *Logging In: Auditing Cybersecurity in an Unsecure World*, 2016 (*www.theiia.org/AuditingCybersecurity*)

Annexe 1 :

Les responsables de l'audit interne les plus performants se distinguent en conseillant leurs parties prenantes

Insurance Australia Group

Jeff Jacobs, responsable de la sécurité des systèmes d'information d'Insurance Australia Group Limited (IAG), supervise l'ensemble de la gestion de la cybersécurité au sein de l'organisation. Afin de réduire l'exposition aux cyberisques d'IAG, il travaille en étroite collaboration avec Lee Sullivan, responsable de l'audit interne, la fonction de gestion des risques de la deuxième ligne de maîtrise, ainsi qu'avec l'équipe chargée de la confidentialité des données.

Lee Sullivan et Jeff Jacobs ont récemment développé une stratégie en matière de cybersécurité. Jeff Jacobs a piloté la conception de cette stratégie, à savoir l'évaluation des capacités existantes, l'identification des risques émergents, la définition dans les grandes lignes des impératifs stratégiques et l'élaboration d'une feuille de route détaillée pour aborder ces risques. Lee Sullivan, quant à lui, a constitué une équipe pour une revue indépendante des premiers résultats de la stratégie quelques temps après sa mise en œuvre. Ils ont convenu d'utiliser un référentiel de cybersécurité identique afin de garantir la cohérence du langage et des messages transmis à la direction générale et au Conseil et ont collaboré tout au long du processus de revue.
Ci-après quelques-uns des défis relevés dans le cadre de l'élaboration de cette stratégie :

- L'importance des fondamentaux — l'exemple le plus éloquent est l'ensemble de principes qui ont été définis pour guider l'organisation dans le choix de ce qui est ou non acceptable du point de vue de la cybersécurité.
- La nécessité d'améliorer la détection et la résolution des incidents, plutôt que de simplement centrer l'attention sur la protection des données — l'époque où l'on pensait qu'il suffisait d'investir dans les outils de protection des données pour éviter les incidents est désormais révolue. Selon Jeff Jacob, la vérité est que « *la protection ne peut jamais être parfaite, c'est pourquoi nous devons renforcer la détection et notre capacité à réagir en cas d'attaque*. »
- La conception de la cybersécurité en amont — bien souvent celle-ci est envisagée après coup. Les concepteurs et les développeurs doivent intégrer la sécurité dans leurs solutions dès le départ.
- La sensibilisation à la cybersécurité — même avec les meilleures technologies, processus et experts, le facteur humain constitue toujours le maillon faible. Le défi consiste à amener les individus à penser à la sécurité afin qu'ils soient davantage conscients des menaces et qu'ils puissent les aborder correctement.

Tous sont d'avis au sein d'IAG que les menaces extérieures sont plus nombreuses et plus sophistiquées chaque jour et qu'un cadre solide de cybersécurité est nécessaire pour faire face à de telles menaces. Toutefois, il n'est pas toujours évident d'estimer les investissements nécessaires pour renforcer les capacités dans ce domaine plutôt que de développer d'autres aspects de la stratégie. Certains au sein de l'organisation, c'est le risque, pourraient craindre qu'en mettant l'accent sur la cybersécurité, on ralentisse le processus de transformation numérique envisagé. Ce que Jeff Jacobs conteste : « *La question n'est pas de savoir si l'on doit opter pour l'un ou pour l'autre, mais plutôt de savoir comment concilier les deux*. »

Université de Virginie

Au sein de l'Université de Virginie, l'équipe de Carolyn Saint, responsable de l'audit interne, Virginia Evans, responsable des systèmes d'information, Jason Belford, responsable de la sécurité des systèmes d'information, Ron Hutchins, vice-président des SI et Gerald Cannon, responsable de l'audit des SI, adopte en matière de sécurité ce que Ron Hutchins qualifie « d'approche en triptyque » pour définir la politique, la mettre en œuvre et auditer sa conformité. L'idée clé est que les fonctions impliquées dans ces différentes étapes restent indépendantes, mais travaillent ensemble. Comme le note Virginie Evans, « *La cybersécurité ne peut fonctionner que si nous travaillons en équipe*. »

Carolyn Saint adopte une approche rigoureuse de l'audit interne afin d'avoir une couverture globale et uniformisée des efforts en matière de cybersécurité et de veiller à ce que l'audit interne vérifie l'efficacité des contrôles, et non pas simplement leur existence. Virginia Evans confirme : « *La précédente équipe d'audit interne ne se souciait que de la conformité. Désormais nous nous attachons davantage à repérer les risques de manière proactive*. »

Jason Belford, Ron Hutchins et Virginia Evans conviennent également que le rôle partenarial et consultatif joué aujourd'hui par l'audit interne est extrêmement bénéfique. Ils envisagent une approche davantage fondée sur le partenariat, avec le sentiment « d'être sur le même bateau », rompant ainsi avec l'image traditionnelle de l'audit interne, qui selon Jason Belford chercherait tous les moyens pour vous discréditer.

Carolyn Saint admet que promouvoir le rôle et la valeur de l'audit interne en matière de cybersécurité auprès des responsables des systèmes d'information et de la sécurité des systèmes d'information demande de la pédagogie ; elle considère toutefois que cela fait partie intégrante des responsabilités du responsable de l'audit interne. Elle ajoute qu'« *il incombe entre autres au responsable de l'audit interne de veiller à ce que la gestion des risques soit considérée comme une propriété à tous les niveaux de l'organisation*. »

Les efforts actuellement engagés par l'université pour se conformer au Federal Information Security Management Act (FISMA) aux États-Unis ont permis de fédérer l'équipe et d'autres représentants des fonctions transversales, autour et au-delà de la question de la cybersécurité. Malgré les progrès réalisés, l'utilisation d'une approche programmatique pour développer un environnement évolutif et pouvoir ainsi répondre aux exigences du FISMA représente un défi considérable.

Pourtant, des efforts conjugués sont indispensables. Comme le souligne Carolyn Saint, « *Les cyberisques sont au premier rang des priorités de tous les plans d'audit et le resteront probablement au cours des prochaines années*. »

Municipalité de Cape Town

L'équipe de la municipalité de Cape Town (Afrique du Sud) considère que la technologie évoluera toujours plus vite que les dispositifs de maîtrise des risques. Il est donc nécessaire de continuer à investir dans le développement de mesures de prévention, de détection et de résolution des incidents.
Même dans cette hypothèse, rien ne garantit de pouvoir échapper aux attaques. Par conséquent, la réussite dépend de la rapidité à laquelle l'équipe peut détecter une faille dans la sécurité et dans quelle mesure elle peut maîtriser les risques en conjuguant efficacité, efficience et rentabilité.

L'équipe réunit Lindiwe Ndaba, responsable de l'audit interne, Etienne Postings, responsable du contrôle des systèmes d'information, et Andre Stelzner, directeur des systèmes d'information et de la technologie. L'approche adoptée en matière de cybersécurité est fondée sur les risques. La priorité est de déterminer la nature des risques SI identifiés
au sein de l'organisation par différentes sources ou prestataires d'assurance. Á cela s'ajoute une discussion approfondie entre l'audit des systèmes d'information et le responsable des systèmes d'information sur les tendances en matière de cyberisques au sein de l'organisation, par rapport aux risques à l'extérieur de l'organisation et aux tendances mondiales susceptibles d'avoir une incidence sur l'organisation.

Andre Stelzner note que pour que la cybersécurité soit couronnée de réussite, chaque membre de l'équipe doit capitaliser sur ses atouts. C'est pourquoi il estime que l'audit interne doit fournir une assurance indépendante sur l'approche adoptée par l'organisation en matière de sécurité, et examiner les règles, systèmes et services mis en place par le service des systèmes d'information pour limiter les risques. Il admet, toutefois, qu'à ce stade, « *nous y parvenons dans une certaine mesure, mais nous nous contentons de vérifier l'adhésion aux règles définies par les systèmes d'information plutôt que d'évaluer la robustesse intrinsèque des mesures de sécurité mises en œuvre*.

L'engagement à travailler en équipe est illustré par l'étroite collaboration entre l'audit interne et l'équipe de sécurité. L'audit interne assiste aux réunions du forum sur la sécurité, qui débat des enjeux communs et élabore des solutions. Tous visent le même objectif : garantir, autant que possible, la sécurité des transactions, des systèmes et des processus.

Se faisant l'écho des propos de Carolyn Saint sur l'importance de la cybersécurité dans les plans d'audit interne, Lindiwe Ndaba et Etienne Postings confirment que dans la municipalité de Cape Town, « *la cybersécurité et l'audit des systèmes d'information feront toujours partie intégrante du plan stratégique de l'audit interne*. »

Annexe 2 :

Etre un conseiller digne de confiance en cybersécurité

En tant que conseiller digne de confiance en cybersécurité, le responsable de l'audit interne est bien placé pour piloter le changement dans l'organisation. Des efforts centrés sur la sensibilisation aux enjeux et leur compréhension, la gestion des risques et les activités d'assurance peuvent l'aider à assumer pleinement ce rôle.

	ÊTRE CONSEILLER DIGNE DE CONFIANCE EN CYBERSÉCURITÉ CE N'EST PAS SEULEMENT...	...C'EST AUSSI...
LA SENSIBILISATION ET DE LA COMPRÉHENSION	Comprendre les concepts, les mécanismes et les éléments de la cybersécurité.	q Développer les compétences actuelles de l'audit des SI pour pouvoir fournir des conseils proactifs et exploitables en matière de cybersécurité. q Conserver des connaissances solides et pratiques sur l'évolution attendue de la réglementation, les nouvelles exigences en matière de couverture d'assurance et les actions collectives en justice récemment intentées et les autres tendances. q S'assurer que les programmes d'audit tiennent compte de ces tendances.
	Collaborer avec les fonctions appropriées au sein de l'organisation pour renforcer la sensibilisation aux enjeux de cybersécurité.	q Fournir des conseils stratégiques aux responsables concernant leur rôle et leurs responsabilités en matière de cybersécurité.
	S'appuyer uniquement sur les équipes SI pour offrir à l'organisation une expertise en cybersécurité.	q Veiller à doter les responsables de l'audit interne et les équipes des compétences requises en cybersécurité via une gestion efficace des talents et des programmes de développement professionnel. q Avoir une approche stratégique de la co-traitance pour s'assurer que les talents et les compétences nécessaires sont disponibles en cas de besoin.

	ÊTRE CONSEILLER DIGNE DE CONFIANCE EN CYBERSÉCURITÉ CE N'EST PAS SEULEMENT...	...C'EST AUSSI...
LE MANAGEMENT DES RISQUES	Conduire une évaluation des risques pour déterminer la probabilité de survenue des cyberisques et leur impact potentiel sur l'organisation.	q Suivre la fréquence et l'ampleur des défaillances en matière de cybersécurité. q Comprendre l'incidence des cybermenaces sur l'organisation et en tenir compte dans le plan d'audit. q Identifier de façon proactive les risques émergents en matière de cybersécurité.
	Se tenir informé de la façon dont l'organisation aborde la cybersécurité et des actions mises en œuvre par le management pour limiter les risques afférents.	q Appréhender l'approche de l'organisation en matière de cybermenaces. q Mettre en œuvre l'audit en continu pour en évaluer la pertinence et l'efficacité des dispositifs de contrôle de la cybersécurité mis en œuvre par le management
	Revoir les évaluations réalisées par les tiers.	q Collaborer avec le responsable des systèmes d'information et le responsable de la sécurité des systèmes d'information pour évaluer les tierces parties potentielles. q Contribuer à l'élaboration du profil de risque des tierces parties potentielles. q Donner des conseils sur la conformité des tierces parties avec la stratégie ou la philosophie de l'organisation en matière de cybersécurité

	ÊTRE CONSEILLER DIGNE DE CONFIANCE EN CYBERSÉCURITÉ CE N'EST PAS SEULEMENT...	...C'EST AUSSI...
ASSURANCE	Évaluer la conformité aux règles et procédures en matière de cybersécurité.	q Fournir une revue indépendante de la stratégie en matière de cybersécurité avant l'élaboration des règles et procédures. q Faire partie intégrante des équipes de mise en œuvre des projets SI pour s'assurer que les cyberisques sont abordés et intégrés en amont, plutôt que gérés après coup. q Comparer et évaluer la pertinence et l'efficacité des règles et procédures au regard de référentiels applicables.
	Évaluer la conformité aux exigences de formation des collaborateurs en matière de cybersécurité.	q Évaluer les résultats des formations et le maintien des connaissances. q Donner des points de vue sur l'alignement de la formation et de la stratégie de l'organisation en matière de cybersécurité.
	Fournir une assurance sur le programme de formation de l'organisation en matière de cybersécurité.	q Capitaliser sur les capacités de l'audit interne et les ressources disponibles au sein de la première et de la deuxième lignes de maîtrise tout en restant objectif. q Piloter les efforts de collaboration en matière de cybersécurité au sein des trois lignes de maîtrise.
	Fournir une assurance sur la résolution des incidents, la reprise après sinistre et les plans de continuité de l'activité.	q Fournir un éclairage sur la coordination des plans et leur alignement sur la stratégie de l'organisation. q Préparer l'audit interne à pouvoir, si besoin, passer à l'action et apporter son aide en cas de crise.
	Faire état des résultats des missions portant sur la cybersécurité au Conseil/comité d'audit.	q Interagir avec la direction et le Conseil/comité d'audit dans le cadre des débats prospectifs en les aidant à passer au crible les failles potentielles de l'organisation. q Contribuer au processus de formalisation de l'appétence aux risques de l'organisation en matière de cybersécurité en donnant des conseils ou en facilitant cet exercice.