PERSPECTIVES INTERNATIONALES

La cybersécurité en 2022 : état des lieux

1RE PARTIE : Les nouvelles propositions de la SEC : un levier de changement

2E PARTIE : Le responsable d'audit interne et le responsable de la sécurité des systèmes d'information (CISO) : un partenariat crucial

3E PARTIE : Cyberincidents : comment les gérer et les surmonter ?

The Institute of Internal Auditors

TABLE DES MATIÈRES

1re partie

Les nouvelles propositions de la SEC : un levier de changement

À propos des experts

Andy Watkin-Child

Andy Watkin-Child possède plus de 20 ans d'expérience dans les domaines de la cybersécurité, de la gestion des risques et de la technologie. Co-fondateur du groupe Augusta – lequel fournit des solutions de gestion, de surveillance et d'assurance en matière de cyber-risques et de cybersécurité – il a travaillé pour des entreprises multinationales dans divers secteurs (ingénierie et fabrication, services financiers, édition et médias), intervenant auprès des équipes de direction en tant que spécialiste des première et deuxième lignes de maîtrise concernant la cybersécurité, la gestion des cyber-risques, le risque opérationnel et les technologies. Il fait en outre partie de plusieurs directoires, équipes de direction mondiales des risques et comités de spécialistes de la cybersécurité, du risque opérationnel et du RGPD (Règlement général sur la protection des données de l'Union européenne).

Manoj Satnaliwala

Manoj Satnaliwala est directeur de l'audit interne au sein du groupe Caliber Home Loans, dont il gère l'ensemble des activités d'audit en collaboration directe avec le comité d'audit. Auparavant, il a dirigé l'équipe d'audit de Radian Group Inc. (troisième plus grande compagnie d'assurance hypothécaire cotée aux États-Unis) et a occupé le poste de directeur de l'audit interne chez PwC. À ce titre, il a notamment été chargé de la validation des contrôles d'audit interne dans le cadre d'une mission d'analyse et d'examen exhaustifs des fonds propres (*comprehensive capital analysis and review*, CCAR) d'un importante groupe bancaire.

Introduction

De futures règles potentiellement lourdes de conséquences

L'actualité 2022 – et celle de ces dernières années, avouons-le – n'est pas des plus rayonnantes. Et sur fond de crise ukrainienne, de pandémie persistante et de tensions sino-américaines croissantes, entre autres, les cybermenaces ne font qu'assombrir le tableau. Dans ce contexte, la cybersécurité est devenue pour l'audit interne un volet majeur – et même prioritaire – de sa cartographie des risques.

Le paysage de la cybersécurité a par ailleurs connu en 2022 des évolutions qui devraient impacter un grand nombre d'organisations et dont les mécanismes et les répercussions vont s'avérer complexes à appréhender. Au premier rang de ces bouleversements figurent deux propositions de règles soumises par la Securities and Exchange Commission (SEC), avec une mention particulière pour la seconde, qui souhaite imposer aux entreprises cotées exerçant leurs activités aux États-Unis de divulguer leurs politiques, leurs procédures et leur stratégie de gouvernance en matière de cybersécurité, ainsi que le degré de connaissance et d'expérience du conseil d'administration dans ce domaine (le cas échéant). Si elles sont adoptées (et l'affaire est en bonne voie), ces nouvelles règles s'appliqueront à toutes les organisations cotées, quelles que soient leur taille et leur secteur d'activité. L'on peut affirmer sans exagération que ces évolutions marquent un nouveau chapitre dans l'histoire de la cybersécurité et constituent un cheval de bataille supplémentaire – quoique pas inconnu – pour l'audit interne qui, face à ce défi, aura un rôle d'accompagnement essentiel à jouer auprès de l'organisation.

Fort heureusement, l'audit interne sait quels sont les outils et les compétences dont il a besoin pour fournir une assurance concernant ce domaine de risque fluctuant qui ne saurait être pris à la légère. Dans cette première partie, nous présentons les nouvelles propositions de la SEC et examinons leur incidence sur la réglementation en vigueur concernant le reporting relatif à la cybersécurité, aux États-Unis et ailleurs. Nous abordons en outre l'importance du rôle des auditeurs internes s'agissant d'aider leur organisation à affronter les perturbations qui pourraient bientôt secouer l'environnement réglementaire.

Poser le décor

La cybersécurité, point culminant du panorama des risques

Un risque aujourd'hui prédominant

Toutes fonctions, toutes organisations et tous secteurs confondus, la cybersécurité demeure résolument inscrite au premier rang des priorités cette année, ainsi que le confirme l'édition 2022 du rapport *North American Pulse of Internal Audit*[1] de l'IIA. En effet, sur les 13 grands domaines de risque soumis à l'appréciation des responsables d'audit interne, la cybersécurité, les technologies de l'information et les relations avec les tiers (qui concernent souvent des prestations informatiques) se partagent le podium. Dans ce trio de tête, la cybersécurité se détache nettement, 85 % des sondés y voyant un risque élevé, voire très élevé, pour leur organisation (alors que, loin en deuxième position, ils sont 61 % à associer un tel niveau de risque aux technologies de l'information).

Ces préoccupations sont justifiées. D'après l'édition 2022 du *SonicWall Cyber Threat Report*[2], l'année 2021 a été le théâtre d'une augmentation alarmante de presque toutes les formes de cyberattaques : +167 % d'attaques cryptées (10,4 millions), +105 % d'attaques par rançongiciel (623,3 millions), +19 % d'attaques de *cryptojacking* (minage malveillant de cryptomonnaie) (97,1 millions), +11 % de tentatives d'intrusion (5 300 milliards), +6 % d'attaques de programmes malveillants visant l'Internet des objets (60,1 millions).

Qui plus est, toutes ces attaques ont des conséquences extrêmement coûteuses. Dans leur almanach 2022 sur la cybersécurité[3], Cisco et Cybersecurity Ventures font en effet état d'un coût total annuel qui pourrait atteindre 10 500 milliards de dollars d'ici à 2025, soit une augmentation de 15 % par an en moyenne.

Et cela sans même tenir compte des mutations drastiques du paysage géopolitique, qui ne sont pourtant pas sans conséquence sur le plan de la cybersécurité. Avant même que la Russie n'envahisse l'Ukraine, les cyberattaques ultra sophistiquées soupçonnées d'être commanditées par le Kremlin s'intensifiaient. Dans l'attaque qui a visé les systèmes de la société texane SolarWinds en 2020, qui aurait été perpétrée[4] par un groupe de pirates dirigé par le Service des renseignements extérieurs de la Fédération de Russie, les systèmes informatiques de près de 18 000 clients[5] – dont Microsoft, Cisco, Intel, Deloitte, le Pentagone, les ministères américains de la Sécurité intérieure et de l'Énergie, et la National Nuclear Security Administration (NNSA) – auraient été secrètement compromis pendant plusieurs mois.

[1]. *2022 North American Pulse of Internal Audit*, The Institute of Internal Auditors, mars 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2]. *2022 SonicWall Cyber Threat Report*, SonicWall, 2022, https://www.sonicwall.com/2022-cyber-threat-report/

[3]. « 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics », Steve Morgan, Cybersecurity Ventures, Cisco, 19 janvier 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/

[4]. « The Russian hacker group behind the SolarWinds attack is at it again, Microsoft says », Joe Hernandez, *NPR*, article mis à jour le 25 octobre 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft

[5]. « The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal », Isabella Jibilian et Katie Canales, *Business Insider*, article mis à jour le 15 avril 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

En 2021, l'entreprise américaine Colonial Pipeline Co.[6] a elle aussi été victime d'une cyberattaque d'ampleur attribuée à Moscou, qui a temporairement interrompu près de la moitié de l'approvisionnement en carburant et en kérosène de la côte Est des États-Unis. Afin de pouvoir restaurer son réseau et récupérer ses données, la compagnie a dû verser près de 5 millions de dollars au groupe de pirates informatiques DarkSide.

Rupture géopolitique

Depuis ces attaques, les inquiétudes à l'égard de la Russie n'ont fait que s'accentuer, pour atteindre un pic avec l'invasion de l'Ukraine, laquelle s'est traduite par des offensives non seulement militaires mais aussi virtuelles, ciblant notamment l'ensemble du réseau électrique ukrainien[7]. Aussi craint-on de plus en plus d'éventuelles représailles suite aux multiples sanctions économiques infligées par l'OTAN et les États-Unis à la Russie. À peine une semaine avant l'incursion russe en Ukraine, la Cybersecurity and Infrastructure Security Agency, aux États-Unis, (CISA) avait publié une déclaration exceptionnelle – intitulée « Shields Up »[8] – recommandant à toutes les entreprises américaines de renforcer leurs dispositifs de cybersécurité et de protection de leurs actifs critiques. « *De récents bulletins d'information publiés par la CISA et d'autres sources non classées révèlent que les pirates agissant sur ordre de la Russie visent les secteurs et entités suivants aux États-Unis et en Occident : centres de recherche sur la COVID-19, gouvernements, organismes électoraux, industrie pharmaceutique, secteurs de la santé, de la défense, de l'énergie, des jeux vidéo, du nucléaire, de l'immobilier commercial, de l'eau, de l'aviation et des équipements de production critiques* », peut-on lire dans une déclaration[9] sur les cybermenaces russes publiée par la CISA en mars 2022.

En mai 2021, Joe Biden a signé un décret (*executive order*)[10] visant à renforcer la sécurité nationale aux États-Unis. Il y souligne notamment la nécessité pour les agences gouvernementales de réviser et étoffer leurs règles et leurs normes en matière de cybersécurité, et pour les organisations de s'attacher à améliorer la sécurité de leur chaîne d'approvisionnement logicielle et leurs mécanismes d'échange d'informations sur les menaces. Plus récemment, le Président américain a publié une déclaration réitérant l'existence de menaces russes à la cybersécurité et rappelant les orientations[11] dynamiques de la CISA sur le sujet.

Le gouvernement russe n'est pas le seul soupçonné de soutenir des cyberattaques déstabilisantes. Selon un rapport[12] publié en 2021 par The Evanina Group, la Chine est de plus en plus active dans le domaine de la cybercriminalité, et notamment dans l'acquisition de données personnelles.

---

[6]. « As Biden warns of a Russian cyberattack, what are the precedents? Here's what happened when a major oil pipeline was hacked last year », Andrew Marquardt, *Fortune*, 22 mars 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/

[7]. « Ukraine foils Russia-backed cyber attack on power grid », Indo-Asian News Service (IANS), 14 avril 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid

[8]. « Shields Up », Cybersecurity & Infrastructure Security Agency (CISA), page consultée le 22 avril 2022, https://www.cisa.gov/shields-up

[9]. « Russia Cyber Threat Overview and Advisories », Cybersecurity & Infrastructure Security Agency (CISA), Department of Homeland Security, page consultée le 22 avril 2022, https://www.cisa.gov/uscert/russia

[10]. « Executive Order 14028: Improving the Nation's Cybersecurity », U.S. General Services Administration (GSA), 12 mai 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity

[11]. « Shields Up », Cybersecurity & Infrastructure Security Agency (CISA)

[12]. *Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP)*, William Evanina, The Evanina Group, 4 août 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf

« *La Chine possède une capacité sans pareille pour dérober notre propriété intellectuelle et nos secrets d'affaires via des méthodes hybrides sophistiquées, aussi bien légales qu'illégales* », constate William Evanina, ancien directeur du National Counterintelligence and Security Center (NCSC).

William Evanina énumère un grand nombre de cyberincidents attribués au Parti communiste chinois, parmi lesquels : la violation de données dont a été victime l'entreprise américaine Equifax en 2017 ; la campagne de piratage menée entre 2011 et 2018 par quatre ressortissants chinois contre une dizaine d'entreprises, d'universités et d'administrations ; les cyberattaques commanditées par l'État chinois entre 2011 et 2013 à l'encontre de compagnies pétrolières et gazières américaines (lesquelles ont fait l'objet d'un rapport publié en juillet 2021 par le ministère américain de la Justice). Il mentionne par ailleurs un rapport conjoint de la National Security Agency (NSA), du Federal Bureau of Investigation (FBI) et de la CISA, publié en juillet 2021 et décrivant une cinquantaine de tactiques et d'outils employés par les pirates informatiques chinois contre les États-Unis.

Compte tenu de la complexité et de la dangerosité de ce cyberenvironnement, la SEC a pris des mesures historiques afin d'aider les organisations à renforcer et à optimiser leur cybersécurité, en durcissant notamment leurs obligations de déclaration à son égard, et, dans certains cas, à l'égard du grand public. Ces mesures sans précédent pourraient avoir des répercussions considérables, non seulement pour les entreprises américaines cotées, mais aussi pour le secteur privé dans son ensemble à travers le monde.

Le Grand Tournant

Une première étape déterminante en matière de déclaration des cyberincidents

Les propositions de la SEC

En l'espace de deux mois, la SEC a dévoilé deux propositions prévues de longue date concernant la cybersécurité en entreprise. La première[13], présentée en février 2022, s'adresse en priorité aux conseillers et sociétés de placement agréés et aux sociétés ou fonds spécialisés en développement commercial. Aux termes des nouvelles règles envisagées, ces derniers seraient ainsi tenus aux obligations suivantes :

- rédiger, adopter et mettre en œuvre des politiques et procédures de cybersécurité visant à gérer les cyber-risques menaçant leur clientèle et les investisseurs ;
- déclarer à la SEC, au moyen d'un nouveau formulaire confidentiel, les cyberincidents affectant un conseiller, un fonds de placement ou des clients ;
- publier, dans leur brochure et leur déclaration d'enregistrement, les cyber-risques et les cyberincidents majeurs survenus au cours des deux derniers exercices.

Les nouvelles règles imposeraient en outre aux conseillers et aux fonds des obligations complémentaires en matière d'archivage, dans le but d'améliorer la disponibilité des informations relatives à la cybersécurité et de faciliter les inspections de la SEC et l'application de ses mesures d'exécution.

« *Les cyber-risques imprègnent de manière transversale la mission de la SEC, déclinée en trois volets, et tout particulièrement ses objectifs de protection des investisseurs et de maintien de l'ordre sur les marchés* », commente le Président de la SEC, Gary Gensler, dans un communiqué de presse[14]. « *Les règles et amendements envisagés visent à améliorer les dispositifs de cybersécurité et pourraient renforcer à la fois la confiance des investisseurs et la résilience des conseillers et des fonds face aux cybermenaces et aux cyberattaques.* »

Si cette première série de règles ne reflète qu'implicitement les attentes de la SEC relatives à la gestion des cyber-risques et à la déclaration des cyberincidents par les entités réglementées, la seconde proposition[15], publiée en mars 2022, les explicite, elle, très clairement. Applicable à l'ensemble des entités cotées, celle-ci a pour but « *d'améliorer et de normer les déclarations des sociétés cotées soumises au* Securities Exchange Act *de 1934 concernant leur gestion des cyber-risques, leur stratégie et leur gouvernance en matière de cybersécurité, et les incidents survenant dans ce domaine* ». Ainsi, les nouvelles règles imposeraient aux sociétés cotées de fournir des informations concernant les aspects suivants :

[13]. *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, U.S. Securities and Exchange Commission (SEC), 9 février 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf

[14]. « SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds », U.S. Securities and Exchange Commission (SEC), 9 février 2022, https://www.sec.gov/news/press-release/2022-20

[15]. *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. Securities and Exchange Commission (SEC), 9 mars 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf

- les politiques et procédures instaurées par l'entreprise pour identifier et gérer les cyber-risques. Les nouvelles règles contiennent une liste détaillée mais non exhaustive des stratégies, politiques et procédures de gestion des risques susceptibles de devoir faire l'objet d'une déclaration. Par exemple :
    - L'entreprise dispose-t-elle d'un programme d'évaluation des cyber-risques ?
    - L'entreprise fait-elle appel à des examinateurs, des consultants, des auditeurs ou d'autres prestataires dans le cadre d'un programme d'évaluation des cyber-risques ?
    - L'entreprise dispose-t-elle de politiques et procédures d'identification et de surveillance des cyber-risques associés au recours à un prestataire ?
    - L'entreprise prend-elle des mesures visant à prévenir et à détecter les cyberincidents et à en limiter les effets ?
    - L'entreprise dispose-t-elle de plans d'urgence, de continuité et de reprise d'activité en cas de cyberincident ?
    - L'entreprise a-t-elle modifié sa gouvernance, ses politiques et procédures ou ses technologies à la suite des cyberincidents qui l'ont affectée ?
    - Les cyber-risques et les cyberincidents dont l'entreprise a été victime ont-ils eu un impact ou sont-ils vraisemblablement susceptibles d'avoir un impact sur son résultat d'exploitation ou sa situation financière ?
    - L'entreprise tient-elle compte des cyber-risques dans sa stratégie générale et dans ses processus de planification financière et de répartition du capital ?

- le rôle de la direction dans la mise en œuvre des politiques et procédures de cybersécurité. Par exemple :
    - Existe-t-il, au sein de la direction, une personne ou un comité chargé(e) d'évaluer et de gérer les cyber-risques ?
    - L'entreprise a-t-elle nommé un responsable de la sécurité des systèmes d'information (ou équivalent) ?
    - Quels sont les processus de signalement des cyberincidents à la personne ou au comité en question, et quels mécanismes de prévention, de détection, d'atténuation et de correction ces derniers appliquent-ils ?
    - La personne ou le comité en question font-ils un rapport sur les cyber-risques au conseil d'administration ou à l'un de ses comités ? Si oui, à quelle fréquence ?
    - La surveillance des cyber-risques est-elle confiée au conseil d'administration dans son ensemble, à certains de ses administrateurs seulement ou à l'un de ses comités ?
    - Le conseil d'administration est-il tenu informé des cyber-risques ? Si oui, à quelle fréquence le sujet est-il abordé ?
    - Le conseil d'administration tient-il compte, lui-même ou par l'intermédiaire de l'un de ses comités, des cyber-risques dans le cadre de sa stratégie générale ou de ses processus de gestion des risques et de contrôle financier ? Si oui, de quelle manière ?

- le niveau d'expertise du conseil d'administration en matière de cybersécurité et son degré de surveillance des cyber-risques. Par exemple :
    - Le conseil d'administration possède-t-il une expérience concrète dans le domaine de la cybersécurité ?
    - Le conseil d'administration possède-t-il une certification ou un diplôme dans le domaine de la cybersécurité ?

- Le conseil d'administration possède-t-il des connaissances, des compétences ou d'autres aptitudes dans le domaine de la cybersécurité ?

En outre, la proposition prévoit un amendement au formulaire 8-K qui imposerait aux sociétés cotées de déclarer tout incident de cybersécurité dans un délai de quatre jours ouvrés, tout comme elles sont déjà tenues de le faire pour les autres imprévus significatifs. L'entreprise concernée devrait notamment indiquer :

- la date à laquelle l'incident a été identifié et s'il est toujours en cours ;
- la nature et l'étendue de l'incident, dans un bref descriptif ;
- si des données ont été volées, altérées, consultées ou utilisées à des fins non autorisées ;
- les conséquences de l'incident sur ses activités ;
- si l'incident a été corrigé ou s'il est en cours de correction.

Selon la SEC, les investisseurs disposeraient alors d'informations « *plus homogènes, plus comparables et donc plus utiles à la prise de décision* ». « *La cybersécurité constitue à présent un domaine de risque émergent avec lequel les émetteurs cotés vont de plus en plus devoir composer* », explique Gary Gensler[16]. « *L'interconnexion de nos réseaux, le recours à l'analyse prédictive et la soif insatiable de données vont grandissant, compromettant la sécurité de nos comptes bancaires, de nos investissements et de nos renseignements personnels. Les investisseurs veulent donc en savoir plus sur la manière dont les émetteurs gèrent ces risques croissants.* »

Une portée historique

À bien des égards, la structure des nouvelles règles envisagées rappelle d'autres règles de la SEC en matière de déclaration, comme celles se rapportant à la situation financière et au résultat d'exploitation (Sarbanes-Oxley), au délit d'initié, ou encore aux forces, faiblesses, opportunités et menaces propres à chaque l'organisation. En revanche, le fait d'imposer une telle obligation de déclaration pour les cyber-risques est totalement inédit.

« *Les États-Unis sont probablement le premier pays, sinon le seul, à réglementer la cybersécurité* », fait remarquer Andy Watkin-Child, co-fondateur du groupe Augusta et de la société Parava Security Solutions, et fondateur de Cybersecurity Maturity Model Certification Europe (CMMC Europe). « *Les entreprises américaines ont peut-être eu affaire au Règlement général sur la protection des données (RGPD) de l'Union européenne et elles pourraient s'empresser de faire le lien entre les deux réglementations. Or, la protection des données et la cybersécurité sont deux paradigmes bien distincts. Ce sont deux choses très différentes et, à part peut-être le règlement sur la gestion financière du ministère de la Défense – en application duquel même les prestataires étrangers pourraient faire l'objet d'une enquête du ministère de la Justice à la recherche de vulnérabilités – il n'existe aucune réglementation comparable dans le domaine de la cybersécurité.* »

Andy Watkin-Child décrit par ailleurs les répercussions non négligeables que ces nouvelles règles pourraient avoir à l'étranger. « *La crise ukrainienne a démontré que la cybersécurité pouvait servir d'arme et, en effet, l'OTAN la considère comme un domaine opérationnel depuis 2016* », explique-t-il. « *La cybersécurité est un outil offensif au même titre que l'arme nucléaire. Le problème, c'est que comme il s'agit d'un domaine opérationnel, elle constitue une lourde menace pour les infrastructures nationales. Les propositions de la SEC toucheront en premier lieu les grands acteurs – les sociétés de courtage, j'entends – mais, selon moi, il y a fort à parier qu'elles déteindront sur des organisations qui ne relèvent pas de la compétence de la SEC, car la communauté internationale des affaires n'a, finalement, pas de frontière.* »

Andy Watkin-Child poursuit en ajoutant qu'en situation de conflit, la cybersécurité doit être envisagée à un niveau global : il suffit d'un seul élément vulnérable pour compromettre directement l'ensemble d'une opération conjointe. Le principe est

[16]. « Statement on Proposal for Mandatory Cybersecurity Disclosures », Gary Gensler, U.S. Securities and Exchange Commission (SEC), 9 mars 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309

le même dans l'univers des entreprises, publiques comme privées. « *Les systèmes d'armement américains ont beau être impénétrables, si les systèmes britanniques peuvent être piratés, alors la protection ne sert plus à rien* », explique-t-il. « *Ce n'est pas sans raison que le Président [américain] a évoqué avec l'OTAN, entre autres sujets, la question de règles de cybersécurité communes. C'est une stratégie judicieuse car, si un pays comme la Russie s'attaque aux entreprises pour couper un réseau électrique, par exemple, alors c'est tout le système d'approvisionnement en eau, en électricité et en gaz qui risque de s'effondrer, sans parler des établissements de santé.* »

De telles répercussions s'entendent évidemment à une échelle macro, mais il ne faut pas non plus négliger les conséquences au niveau micro, c'est-à-dire pour chaque organisation. Des effets qui, malgré ce que l'on pourrait penser en voyant la longue liste d'informations qu'il conviendrait d'intégrer dans les déclarations sur la cybersécurité, ne sont pas tous si incommodants.

« *Certes, cette déclaration est avant tout une obligation légale* », concède Andy Watkin-Child, « *mais, comme il est précisé dans les propositions, ces informations ne sont pas destinées qu'à la SEC ; elles s'adressent également à l'ensemble des acteurs du marché susceptibles d'avoir une influence sur l'entreprise. Investisseurs, agences de notation de crédit, compagnies d'assurances... Tous vont pouvoir, comme la SEC, apprécier son expertise, ou inexpertise, en matière de cybersécurité. Une telle transparence comporte inévitablement un risque, mais elle est aussi source d'opportunités.* »

L’audit interne : un rôle qui demeure constant

Identifier, évaluer, communiquer

Des acquis à exploiter

La loi Sarbanes-Oxley de 2002 (SOX) a assigné des responsabilités supplémentaires à la fonction d’audit interne, lui offrant la possibilité d’apporter encore plus de valeur ajoutée à l’organisation. En effet, pour des organisations qui tentaient de se familiariser avec la nouvelle législation, l’audit interne est souvent devenu un expert en conformité SOX. Au vu de la teneur des récentes propositions de la SEC, il y a fort à parier que la fonction endosse cette fois-ci un rôle d’expert en cybersécurité.

Étant donné la complexité de cette thématique, cela semble à première vue impossible, du moins sur le court terme. D’après les résultats de l’enquête *Pulse*[17], la cybersécurité représente en moyenne seulement 9 % du plan d’audit dans les organisations cotées. C’est 2 points de pourcentage de plus que ces trois dernières années, mais très loin de la part allouée au reporting financier (35 %). Plusieurs raisons peuvent expliquer ce chiffre, comme un budget limité, des ressources insuffisantes, ou encore une méconnaissance du sujet ou un manque d’expérience.

Toutefois, la valeur ajoutée que l’audit interne peut apporter ne tient pas tant à sa connaissance du domaine de la cybersécurité, mais plutôt à son expertise en matière d’identification et de communication des risques, ainsi qu’en matière d’évaluation des dispositifs de contrôle associés à la gestion des risques. Ce sont là en effet les aspects sur lesquels insiste la SEC dans ses propositions sur un type de risques en particulier.

« *Il faut bien comprendre que ces propositions ne portent pas sur la cybersécurité à proprement parler, mais sur la gestion des cyber-risques* », fait observer Andy Watkin-Child. « *Dès qu’il est question de cybersécurité, les gens ont tendance à penser qu’il s’agit de mettre en place des dispositifs de contrôle et d’apporter des correctifs. Or, ce n’est pas du tout ce que la SEC demande ; son objectif est d’inciter les organisations à évaluer leurs cyber-risques. Elle préconise donc au conseil d’administration d’instaurer une structure de gouvernance adéquate pour évaluer et superviser le programme de gestion des cyber-risques de l’organisation, quelle qu’en soit la forme.* »

« *Ce que désire la SEC, c’est que le conseil d’administration assume son rôle de supervision et d’assurance* », indique Manoj Satnaliwala, responsable de l’audit interne chez Caliber Home Loans, Inc. « *Le problème ne vient pas d’un quelconque manque de règles, puisqu’il existe bel et bien des cadres de référence pour guider les organisations, tels que le Cadre de cybersécurité du National Institute of Standards and Technology (NIST). Le fond du problème, c’est la désignation des responsabilités, qui peut vite tourner au jeu de ping-pong.* »

Or, l’audit interne peut contribuer à rétablir un certain équilibre. « *Le conseil d’administration et la direction ont besoin d’aide. Grâce à son rôle d’assurance, l’audit interne est garant du devoir de rendre compte et, parce qu’il a une meilleure visibilité de l’ensemble de l’organisation, il favorise la prise de responsabilité partagée vis-à-vis des risques* », explique Manoj Satnaliwala. « *Peu importe la nature du risque considéré, le rôle de la fonction d’audit interne, lui, demeure constant. La fonction n’a donc pas besoin de partir de zéro. Mais, si l’on ne peut raisonnablement pas s’attendre à ce qu’elle maîtrise toutes les subtilités d’un programme de cybersécurité, il s’agit malgré tout d’aller au-delà de la simple compréhension des propositions de la SEC et de ses attentes. À partir du moment où l’organisation possède au moins quelques ressources*

[17]. *2022 North American Pulse of Internal Audit*, The Institute of Internal Auditors

compétentes en cybersécurité, je ne pense pas que la fonction d'audit interne doive changer quoi que ce soit, si ce n'est ajuster en conséquence son périmètre de couverture des risques. »

Pour l'organisation, cependant, accéder à de telles ressources est souvent loin d'être une sinécure. Toutes les formations et certifications du monde ne lui permettront pas d'acquérir une expertise en cybersécurité du jour au lendemain. Les petites fonctions d'audit interne qui n'ont pas les moyens de recruter des talents prisés et coûteux, en particulier, ont peu de solutions pour élargir leur rôle au-delà d'une simple vérification de la conformité aux processus. C'est pourquoi l'audit interne doit savoir exactement où chercher les experts les plus accessibles. Deux options s'offrent à lui :

- **Puiser au sein même du vivier de talents de l'organisation.** Ceux qui peuvent faire valoir une expérience en audit informatique traditionnel possèdent souvent les connaissances de base pour achever rapidement une formation technique en cybersécurité. En outre, certains fondamentaux de la cybersécurité peuvent servir dans des domaines tels que la gestion du changement, les contrôles des accès, les activités informatiques ou encore les opérations de reprise après sinistre, ce qui, sur le long terme, réduirait la nécessité d'externaliser.
- **Collaborer avec la deuxième ligne et des fonctions d'audit externe de confiance.** S'il est essentiel de préserver l'indépendance et l'objectivité de l'audit interne, conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne*, le fait de collaborer plus étroitement avec les fonctions qualifiées telles que le service informatique peut permettre aux auditeurs d'avoir accès à des compétences techniques potentiellement difficiles ou onéreuses à acquérir à l'extérieur.

Conclusion

Préparez-vous !

La cybersécurité est un domaine en constante évolution dans lequel les entreprises ne cessent d'innover pour déjouer des cyberattaques toujours plus élaborées. Cependant, dans l'histoire de la cybersécurité, l'année 2022 marquera assurément un tournant du fait des étapes franchies pour contrer les tendances alarmantes observées dans le milieu des entreprises. Bien que les propositions de la SEC doivent encore faire l'objet d'une période de consultation de 60 jours, la version officielle qui sera publiée ne devrait pas trop surprendre les entreprises cotées et leur fonction d'audit interne.

Si ce n'est déjà fait, l'audit interne peut et devrait utiliser le temps dont il dispose pour inventorier l'ensemble des éléments de l'organisation à prendre en compte dans la stratégie de cybersécurité. Sans ce travail, les auditeurs internes peineront à évaluer les dispositifs de contrôle, les politiques et les stratégies de gouvernance en place en matière de cybersécurité. Or, cette évaluation est importante tant pour la sécurité de l'organisation que pour celle du marché tout entier. Le monde devient toujours plus interconnecté. Aussi les responsabilités relatives aux risques tels que les risques cyber sont-elles largement partagées. Et comme l'histoire l'a démontré à maintes reprises, le piratage d'une seule organisation peut avoir un véritable effet domino.

Une chaîne n'est aussi solide que son maillon le plus faible.

2E PARTIE

Le responsable d'audit interne et le responsable de la sécurité des systèmes d'information (CISO) : un partenariat crucial

À propos des experts

Jerry Perullo

Jerry Perullo est le fondateur de la société Adversarial Risk Management, qui accompagne les entreprises en pleine croissance dans la mise en place de programmes de cybersécurité avancés. Avant de créer sa société, il a été pendant près de 20 ans responsable de la sécurité des systèmes d'information chez Intercontinental Exchange (NYSE : ICE), où il a conçu et piloté le programme de cybersécurité d'infrastructures économiques majeures, dont la Bourse de New York. Titulaire de la certification délivrée aux administrateurs par la National Association of Corporate Directors (NACD Directorship Certification®), Jerry Perullo a en outre siégé au conseil d'administration du Financial Services Information Sharing and Analysis Center (FS-ISAC) pendant six ans, en dernier lieu en qualité de président. Il enseigne par ailleurs à la School of Cybersecurity and Privacy du Georgia Institute of Technology et partage ses expériences avec d'autres spécialistes des risques technologiques via sa série de podcasts #lifeafterCISO.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal occupe un poste de directeur d'audit interne à Dubaï. L'Institute of Internal Auditors (IIA) le classe parmi les 15 principaux leaders mondiaux de moins de 30 ans. Titulaire d'une licence (BBA) et d'un master (MBA) en administration des entreprises et d'un diplôme d'études sur le Moyen-Orient, Hassan NK Khayal est également certifié CIA (Certified Internal Auditor), CRMA (Certification in Risk Management Assurance) et CFE (Certified Fraud Examiner), et cumule les certifications professionnelles dans divers domaines : robotisation des processus (RPA), analyse de données, Internet des objets, gestion de la qualité, santé et sécurité, gestion environnementale et gestion des risques.

Alan Maran

Alan Maran est directeur de l'audit interne chez Chewy, Inc. depuis janvier 2019. Sa mission consiste à superviser l'ensemble des activités de la fonction d'audit interne sur le plan de la stratégie et de l'exécution, à savoir : évaluations des risques de l'entreprise en mode « Agile » ; appui aux activités ; assurance sur l'adéquation des dispositifs de contrôle relatifs aux principaux risques pesant sur l'organisation ; alignement, à l'échelle de l'entreprise, avec les opérations, les systèmes internes et les processus de gouvernance, de gestion des risques et de conformité (GRC) dans le domaine informatique ; suivi continu de l'évolution professionnelle des équipes d'audit interne et accent sur certaines compétences prioritaires (analyse de données, cybersécurité, confidentialité des données). Fort de plus de 22 ans d'expérience au sein de la *fintech*, du commerce électronique, des technologies et de l'industrie manufacturière, Alan Maran est un cadre aguerri, à la curiosité insatiable. Il a débuté sa carrière chez Ernst & Young, LLC puis a occupé différents postes d'audit interne au sein de multinationales du classement Fortune 500 avant de rejoindre Chewy. Titulaire d'un master en administration des entreprises (MBA) et d'un master en finances de l'Université de l'État de Washington, il est aussi certifié CFE (Certified Fraud Examiner) et CBE (Certified Blockchain Expert) et membre de chapitres locaux de l'IIA.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan est directeur des données et de la sécurité des systèmes d'information chez Chewy, Inc. Il a rejoint la société en octobre 2019 en tant que responsable de la sécurité, des données et des systèmes internes. Sa mission consiste à superviser la sécurité des systèmes d'information, la gestion des plateformes d'analyse de données, les systèmes internes ainsi que les processus de gouvernance, de gestion des risques et de conformité dans le domaine informatique à l'échelle de l'entreprise. Fort de plus de 25 ans d'expérience acquise dans les secteurs du commerce électronique, des services bancaires et financiers, et de la distribution et du marketing, Srini Srinivasan est expert en nouvelles technologies. Avant de rejoindre Chewy, il a occupé plusieurs postes de direction chez Citizens Financial Group, Inc. Il est titulaire d'un master en informatique de l'Université Bharathidasan et d'un master en administration des entreprises (MBA) de l'Université de Bentley.

Introduction

Les partenariats autour de la cybersécurité : un facteur clé de réussite

Les cyber-risques demeurent prédominants pour toutes les organisations. Toutes les études montrent que les cybercriminels s'emploient inlassablement à pirater en toute impudence des données sensibles ou à forcer des personnes inexpérimentées et sans méfiance à divulguer de telles données ou à leur en fournir l'accès.

Par exemple, le rapport d'investigation 2022 de Verizon sur les violations de données fait état d'une hausse de 13 % des attaques par rançongiciel en 2021. C'est plus que ces cinq dernières années cumulées. Les méthodes les plus infaillibles restent pourtant les mêmes : utilisation détournée des logiciels de partage de bureau et d'accès à distance (40 %) et intrusion par messagerie électronique (35 %)[18].

Le nouveau GTAG (*Global Technology Audit Guide*) de l'IIA, intitulé *Auditing Cybersecurity Operations: Prevention and Detection*, recommande aux organisations d'examiner leurs activités de cybersécurité, et de donner la priorité à une assurance concernant ces dernières. Il sert également de guide aux auditeurs internes, pour les aider à définir le périmètre des activités de cybersécurité, à en identifier les composantes, à appliquer les recommandations les plus pertinentes extraites des cadres de référence sur les contrôles informatiques, et à se familiariser avec les approches en matière d'audit de la cybersécurité.

En revanche, le GTAG ne couvre pas l'importance d'une relation saine entre le responsable d'audit interne et le responsable de la sécurité des systèmes d'information (CISO). Une bonne coordination entre ces deux experts faciliterait, d'une part, l'alignement de l'audit interne et de la sécurité des systèmes d'information au sujet des cadres de référence, des activités de gestion des risques et des dispositifs de contrôle, et, d'autre part, la gestion du profil évolutif des cyber-risques.

Dans cette deuxième partie, nous analysons les avantages d'un partenariat étroit entre le responsable d'audit interne et le responsable de la sécurité des systèmes d'information. Nous examinons en outre comment il est possible d'établir et d'entretenir une telle collaboration tout en préservant l'indépendance de l'audit interne, et évaluons la valeur ajoutée que cette alliance représente pour l'organisation.

[18]. « 3 Takeaways From the 2022 Verizon Data Breach Investigations Report », Jesse Mack, *Rapid7*, 31 mai 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/

Arguments en faveur d'un engagement collectif en matière de cybersécurité

Cyber-risques : un enjeu transversal

La cybersécurité est un domaine de risque évolutif et croissant avec, chaque année, des cyberattaques toujours plus nombreuses et sophistiquées. Les statistiques ne manquent pas pour montrer à quel point les organisations, tous secteurs confondus, demeurent vulnérables. Parallèlement, celles-ci adoptent des stratégies fondées sur les données (collecte, gestion, analyse et utilisation) et exploitent les nouvelles technologies pour gagner en performance et en rentabilité.

Tout comme les autres domaines de risque significatifs, les cyber-risques devraient être appréhendés et gérés à l'échelle de l'organisation tout entière. Pourtant, rares sont les organisations qui adoptent une approche aussi globale. Tel est le constat qui ressort du rapport *The State of Cyber Resilience* publié par Microsoft et Marsh (société spécialisée en gestion des risques et courtage en assurances). Selon ce dernier[19], établi à partir d'une enquête réalisée auprès de plus de 600 spécialistes des cyber-risques, seules 4 organisations sur 10 impliquent leurs services juridique, planification, finances, opérations ou gestion de la chaîne logistique dans l'élaboration de leur plan de gestion des cyber-risques[20].

« *L'un des freins à la confiance réside dans le fait que la plupart des entreprises n'ont pas encore adopté d'approche globale en matière de gestion des cyber-risques, c'est-à-dire une approche qui, fondamentalement, repose sur une communication large et favorise la collaboration et le consensus entre les différentes parties prenantes durant les prises de décision importantes au sujet de la cyber-résilience*[21] », peut-on lire dans le rapport.

Plusieurs grandes tendances y sont mentionnées :

« *N'importe quelle organisation peut être la cible d'une cyberattaque. Aussi les objectifs de cybersécurité (mesures, assurance, analyses de données et plans de résolution) doivent-ils être alignés à l'échelle de l'organisation afin que celle-ci puisse renforcer sa cyber-résilience et non simplement prévenir les incidents.* »[22]

Le responsable d'audit interne peut grandement contribuer à la mise en œuvre d'une approche globale efficace, en établissant avec le CISO une relation durable fondée sur des objectifs communs, une compréhension réciproque et un respect mutuel.

D'après Jerry Perullo, fondateur de la société Adversarial Risk Management et ancien CISO de la société mère de la Bourse de New York (Intercontinental Exchange, NYSE : ICE), une communication médiocre ou un manque de compréhension entre le responsable d'audit interne et le CISO peuvent compromettre les chances d'adopter une approche commune en matière de cybersécurité. *A contrario*, une bonne relation favorise une meilleure compréhension des objectifs, de la stratégie, des activités et des politiques de chacun, mettant ainsi en avant la valeur ajoutée de l'audit interne – et, par extension, de ses constats et ses recommandations – pour les responsables des cyber-risques, la direction générale et le conseil d'administration. En outre, les deux fonctions ont ainsi la possibilité d'en apprendre davantage sur leurs missions respectives et sur la contribution de chacune à la stratégie globale de cybersécurité.

[19]. Enquête mondiale 2022 Marsh et Microsoft sur les risques cyber
[20]. *The State of Cyber Resilience*, Marsh et Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience
[21]. Ibid.
[22]. Ibid.

« *En fin de compte, ce que souhaite l'audit interne, c'est découvrir l'univers de la sécurité des systèmes d'information* », constate Jerry Perullo. « *Il existe de nombreuses façons de procéder, mais la meilleure, c'est encore de se tourner vers les experts eux-mêmes.* »

Lorsqu'il intervient comme consultant auprès de start-up, Jerry Perullo commence généralement par leur faire instaurer un programme de gouvernance en matière de cybersécurité. En principe, cela consiste à créer un comité de gouvernance pluridisciplinaire, composé de membres de la direction générale et de représentants des équipes juridique, finances et sécurité des systèmes d'information. Des responsables d'audit interne seniors y participent souvent à titre d'observateurs.

Cinq facteurs clés de réussite

Les avantages d'une relation étroite entre le responsable d'audit interne et le CISO

Un partenariat bien rodé entre le responsable d'audit interne et le CISO comporte de nombreux avantages. Si les modalités d'une telle collaboration peuvent varier en fonction de la taille de l'organisation, de son profil de cyber-risques ou encore du niveau de réglementation de son secteur d'activité, on distingue tout de même cinq domaines dans lesquels elle peut s'avérer bénéfique en toutes circonstances :

Appréhender et assimiler le profil de cyber-risques de l'organisation

Un profil de risques consiste en une analyse quantitative des différents types de menaces qui pèsent sur l'organisation. En matière de cybersécurité, cette analyse permet d'identifier les actifs critiques et les cyber-risques, d'examiner les politiques et les pratiques visant à gérer ces risques, et d'appréhender les éventuelles vulnérabilités. Connaître le profil de cyber-risques de l'organisation permettrait à l'audit interne non seulement d'élaborer un plan d'audit cohérent avec l'approche globale poursuivie en matière de cybersécurité, mais aussi d'accroître sa pertinence et sa valeur ajoutée dans ce domaine clé.

Au cours des trois années qui ont suivi l'introduction en bourse de Chewy, Inc. (société spécialisée dans la vente en ligne d'aliments et autres produits pour animaux de compagnie), Alan Maran et Srini Srinivasan, respectivement directeur de l'audit interne et CISO de la société, ont noué une relation étroite. Srini Srinivasan explique s'être associé avec l'audit interne, la fonction juridique et d'autres acteurs afin de pouvoir évaluer de manière transversale le profil de cyber-risques de la société au regard du Cadre de cybersécurité du National Institute of Standards and Technology (NIST).

« *C'était notre point de départ* », commente Srini Srinivasan. « *Nous avons ensuite élaboré une feuille de route sur trois ans pour la cybersécurité et la gouvernance, que nous avons ajustée et améliorée en fonction de notre évaluation du cadre de cybersécurité. Nous procédons désormais à une évaluation chaque année afin de mesurer notre progression dans ces domaines ainsi que l'évolution de notre score de risque global.* »

Cette approche collaborative impliquant d'entrée de jeu l'audit interne a permis d'élaborer une stratégie mutuelle intégrant ses services d'assurance et de conseil, l'objectif étant d'améliorer continuellement le dispositif de cybersécurité global de Chewy.

« *Nous ne nous contentons pas d'auditer les systèmes informatiques et de sécurité. Notre tâche consiste également à épauler Srini et son équipe dans le développement d'une stratégie globale* », explique Alan Maran.

Autre avantage de cette collaboration, souligné par Srini Srinivasan : les concepts de « sécurité des systèmes d'information » et d'« assurance indépendante » sont tout de suite pris en compte dans les nouveaux projets. Autrement dit, la sécurité des systèmes d'information, l'audit interne et les dispositifs de contrôle relatifs à la gouvernance ne sont plus les parents pauvres de l'histoire.

Il poursuit : « *Ce que nous faisons au moment du lancement d'un nouveau projet, c'est que nous nous entretenons, mon équipe et celle de l'audit interne, avec les équipes techniques, produits, commerciales et d'autres encore, afin de déterminer quels sont les aspects de sécurité à prendre en compte et si nous suivons bien les bonnes pratiques.* »

Srini Srinivasan précise que cette démarche leur permet d'identifier, de limiter, voire, dans la mesure du possible, d'éliminer les cyber-risques, grâce à la mise en place de processus et de dispositifs de contrôle adaptés au fil de la conception du projet. « *Ainsi, lorsque le projet démarre, nos équipes ne sont pas dépassées car elles en ont toutes deux une parfaite*

maîtrise. Lorsque nous effectuons un suivi au moyen d'évaluations des contrôles d'audit, d'examens des accès ou de contrôles de gouvernance, nous comprenons mieux ce que nous faisons. »

Comprendre le rôle de chacun

Le fait que Chewy soit une société cotée depuis relativement peu a grandement facilité la relation bâtie par Alan Maran et Srini Srinivasan dans la mesure où cela leur a permis de partir d'une page blanche avec, en perspective, des échanges transparents et fréquents entre les deux responsables et leurs équipes respectives.

« *C'était un moyen idéal pour instaurer confiance et transparence auprès des principaux acteurs ; nous ne voulions surtout pas manquer cette occasion* », raconte Srini Srinivasan.

Il reconnaît cependant qu'Alan Maran et lui ne sont pas pour autant toujours sur la même longueur d'onde. Seulement, en cas de désaccord, leur relation facilite la discussion et ils parviennent à trouver une solution qui convient à tous.

« *Je n'ai absolument aucun intérêt à tenir les auditeurs internes à l'écart* », confie-t-il. « *Plus ils en sauront sur notre métier, meilleure sera leur capacité d'évaluation. Et je ne pense pas me tromper en disant qu'il n'y a aucune rivalité entre nous.* »

Srini Srinivasan constate que cette approche collaborative offre finalement une certaine agilité dans la mesure où l'audit interne fait partie intégrante d'un processus dans lequel les déficiences peuvent être détectées et traitées précocement.

Alan Maran ajoute que ce partenariat ouvert appuie et renforce leur compréhension mutuelle du rôle de chacun.

« *Srini ne fait pas comme si on savait tout sur tout, et, qui plus est, il respecte nos préoccupations et nos points de vue* », révèle-t-il.

Faire valoir son utilité

Apporter un éclairage et des constats d'assurance sur des sujets critiques au moment propice constitue l'un des plus grands défis de l'audit interne dans n'importe quel domaine de risque, et plus encore dans celui de la cybersécurité, qui, parce qu'il évolue à un rythme effréné, nécessite une assurance à la fois pertinente et à point nommé.

Jerry Perullo met en garde contre les missions et recommandations d'audit interne qui ne seraient pas en ligne avec la mission de cybersécurité de l'organisation, en ce qu'elles pourraient causer plus de tort que de bien. Elles peuvent en effet semer la confusion au sein de l'équipe en charge de la sécurité des systèmes d'information, surtout si l'audit interne est indécis sur les informations qu'il souhaite consulter.

« *L'audit interne peut ne pas savoir exactement dès le départ ce qu'il recherche* », explique-t-il. « *Il vaut donc mieux collaborer avec lui en amont et suivre le processus de cybergouvernance afin de garantir que sa mission soit bien en ligne avec la nôtre.* »

Selon Hassan Khayal, consultant en audit interne et expert en cybersécurité, il s'agit d'un domaine dans lequel l'audit interne prête tout particulièrement le flanc aux critiques. Trop souvent, les auditeurs internes s'abstiennent de rencontrer des membres de l'équipe informatique ou de la sécurité des systèmes d'information et d'en apprendre davantage sur le sujet sous prétexte de protéger leur indépendance.

« *Personnellement, lors de mes premières missions, je n'ai eu aucune honte à avouer aux collaborateurs de l'équipe informatique que j'étais plus là pour apprendre qu'autre chose. Je leur ai posé des questions sur leurs processus et leurs techniques et ils m'ont gentiment expliqué les tenants et les aboutissants de leur métier autour d'un déjeuner.* »

Hassan Khayal ajoute que ce type de formation peut également permettre aux auditeurs internes de mieux apprécier le degré de maturité de l'organisation en matière de cybersécurité, ce qui leur est essentiel pour formuler des recommandations pertinentes.

« *Pour une PME, ou même une grande entreprise non cotée, il y a des limites à ce que l'on peut ou à ce que l'on doit faire* », précise-t-il. « *À un certain stade, vos recommandations peuvent s'avérer trop agressives et donc devenir complètement irréalistes.* »

Le fait d'instaurer une solide relation entre les équipes d'audit interne et de sécurité des systèmes d'information permet de limiter les risques de missions et de recommandations d'audit inutiles ou malavisées. Un avantage qui s'est vérifié chez Chewy.

« *Alan et les membres de son équipe sont intarissables sur notre stratégie de sécurité globale, technologiquement parlant, ainsi que sur nos activités et nos principaux risques* », raconte Srini Srinivasan. « *Les notations des risques et nos capacités internes sont parfaitement alignées. Nous allons donc pouvoir continuer à étoffer nos connaissances, ainsi que celles de nos collègues et de nos dirigeants.* »

Communiquer avec le conseil d'administration et la direction générale

La culture d'entreprise de Chewy offre une meilleure visibilité sur les risques, favorisée par des discussions ouvertes. Alan Maran et Srini Srinivasan ont entrepris de sensibiliser les parties prenantes (à savoir, la direction générale et le conseil d'administration) quant aux bienfaits de leur collaboration.

« *Dans bon nombre d'organisations, la tendance est au cloisonnement. Autrement dit, en cas de problème concernant la sécurité informatique, le premier réflexe consiste à solliciter le CISO. Mais dans le cadre d'une démarche de gestion intégrée des risques ou de management des risques de l'entreprise, le moindre risque identifié concerne l'ensemble de l'organisation* », indique Alan Maran. « *Une cyberattaque peut avoir des répercussions sur vos activités, vos livrables et vos finances. Srini a fait un excellent travail de sensibilisation de la direction à nos actions et aux risques que nous traitons. De ce point de vue, on peut donc bel et bien parler de collaboration.* »

Cette démarche permet en outre de s'adapter avec rapidité et souplesse aux mutations du panorama des risques et du cadre réglementaire. Par exemple, Alan Maran et Srini Srinivasan sont plus que convaincus que leur organisation est en mesure de satisfaire aux futures obligations de déclaration en matière de cybersécurité présentées par la SEC début 2022.

Par ailleurs, leur collaboration ne se limite pas aux seuls domaines de la sécurité des systèmes d'information et de l'audit interne. « *La sécurité de l'organisation n'est pas notre seul cheval de bataille* », confie Srini Srinivasan. « *Il y a d'autres acteurs clés avec lesquels nous avons noué des partenariats similaires, comme les équipes comptables ou encore les équipes juridiques. Pour moi, ces relations transparentes nous mettent dans de très bonnes dispositions pour affronter les exigences réglementaires à venir.* »

Soulignant que la direction de Chewy bénéficie d'une communication cohérente concernant la situation et les besoins de l'organisation en matière de cybersécurité, Hassan Khayal met en garde contre les risques non négligeables qui pourraient découler de l'absence d'une telle communication. Selon lui, des dirigeants mal informés pourraient très vite voir l'informatique et la cybersécurité comme un simple coût. Il ajoute que si l'audit interne ne fait pas l'effort de se former à la sécurité des systèmes d'information, il a peu de chance de pouvoir apporter une assurance utile et pertinente dans ce domaine, ce qui risque d'altérer l'opinion de la direction générale et du conseil d'administration.

Respecter et préserver l'indépendance de l'audit interne

Hassan Khayal, qui brigue actuellement la certification CISA (Certified Information Systems Auditor), affirme que cette initiative a d'ores et déjà renforcé sa crédibilité auprès des professionnels de l'informatique et de la sécurité des systèmes d'information. Cela lui a également permis d'échanger avec eux sur un pied d'égalité et de s'assurer qu'il pourra, si besoin, avoir accès à des informations souvent jugées trop complexes pour des auditeurs « de passage » qui ne sont là que pour mener à bien leur mission d'audit. Qui plus est, ces échanges ne compromettent ni son indépendance ni son objectivité.

« *Il ne faut pas oublier que l'on est tout de même sur un lieu de travail* », fait-il remarquer. « *Lorsqu'on dit à un auditeur de préserver son indépendance, je ne pense pas que cela signifie qu'il ne peut pas être ami avec ses collègues et qu'il doit déjeuner tout seul.* »

Hassan Khayal confirme adopter cette approche avec tous les services de l'organisation. Il discute Linux avec ses collègues de l'informatique, réseaux sociaux avec l'équipe marketing, etc.

« *C'est un bon moyen d'étoffer et d'entretenir ses connaissances professionnelles, tout comme son réseau* », confie-t-il. « *C'est exactement comme quand nous assurons à nos clients d'audit que nous allons examiner tel processus ou telle opération, mais pas leurs collaborateurs. Du coup, si vous sortez déjeuner avec un collaborateur, vous oubliez le processus ou l'opération en question.* »

Chez Chewy, la relation étroite entre Alan Maran et Srini Srinivasan favorise une compréhension mutuelle de l'obligation d'indépendance.

« *Notre profession repose sur un principe simple : faire confiance mais vérifier. Par souci d'objectivité, j'ai le devoir d'appliquer ce principe* », explique Alan Maran. « *Alors oui, nous faisons confiance jusqu'à un certain point, en particulier pour les choses que nous testons régulièrement. Dans la plupart des cas, nous confirmons que rien n'a changé. Pour autant, je continue aussi d'évaluer l'intégrité des informations fournies par la direction. Nous ne prenons pas pour argent comptant les rapports soumis à notre examen. Nous remontons jusqu'à la source pour vérifier leur exactitude et leur exhaustivité et être sûrs que nous obtenons les mêmes résultats.* »

Alan Maran concède que le fait de mieux connaître le rôle de chacun au sein de l'organisation facilite grandement les choses.

« *Nous travaillons en bonne intelligence. J'ai une mission et une assurance à apporter à la direction générale, au conseil d'administration, au comité d'audit et aux autres parties prenantes* », dit-il. « *Aussi, nous tâchons de nous accorder sur le plan d'audit annuel et sur le périmètre. Bien sûr, il nous arrive parfois d'avoir des divergences de vue, mais nous sommes rarement en désaccord sur les domaines de risque qui nécessitent une assurance.* »

Srini Srinivasan ajoute que pour mener à bien une approche fondée sur les données en matière de cybersécurité, les équipes de sécurité des systèmes d'information et d'audit interne doivent s'accorder sur les faits.

« *En cas de désaccord, nous devons tâcher de trouver une solution pour parvenir à un consensus* », explique-t-il. « *Il peut alors y avoir une part de subjectivité sur le degré de criticité perçu par chacun – faible, moyen ou élevé. Un dialogue de sourds ne nous mènera à rien, contrairement à une discussion franche et à un cadre de référence commun.* »

Vers plus de valeur ajoutée

Une cyber-résilience renforcée

Srini Srinivasan a toujours eu à cœur de rester fidèle à la mission de Chewy. Son objectif est donc triple : appliquer les principes de fonctionnement interne de la société, garantir l'alignement des fonctions de sécurité de l'information et d'audit interne, et mettre la transparence au service de la confiance.

« *Je trouve que nous avons fait énormément de progrès et que cette stratégie porte réellement ses fruits quand on la rapporte aux efforts minimes que les équipes et la direction doivent déployer pour se tenir mutuellement informées* », constate-t-il.

Nous l'avons dit, la mise en œuvre d'une approche souple, associant l'audit interne de manière continue au processus de cybersécurité, repose sur une communication, une collaboration et une coopération de qualité. Srini Srinivasan fait observer que les grandes tendances actuelles – telles que l'attention croissante portée au développement durable, à la chaîne logistique, aux conditions du marché, au climat géopolitique, etc. – nécessitent une approche résiliente de la cybersécurité et de l'assurance associée.

« *Toutes ces tendances nous obligent à être vigilants, habiles, réactifs et pertinents* », reconnaît-il. « *Car si nous adoptons une approche en cascade classique, avec des délais d'exécution plus longs, nous risquons de manquer le coche. Je suis donc on ne peut plus ravi de notre niveau d'échange.* »

Des connaissances étoffées

Autre avantage inhérent à ce type de partenariat : chaque équipe évolue et progresse dans la compréhension et l'appréciation de l'approche de l'autre vers la réalisation de leur objectif commun, à savoir garantir la cybersécurité de l'organisation.

« *Nous vérifions systématiquement l'expertise technique de l'autre, notamment en nous demandant si tel élément a été examiné, si tel aspect a été pris en compte, ou si nous sommes d'accord sur telle analyse de risque* », raconte Alan Maran. « *Dès le départ, nous définissons notre feuille de route et Srini participe aux réunions de lancement. Il est impliqué avant même le démarrage de la mission d'audit, de sorte qu'il n'y ait absolument aucune surprise.* »

Mais la vraie valeur ajoutée de cette collaboration ne transparaît véritablement que lorsque la mission débute et que l'audit interne travaille directement avec le personnel informatique et de la sécurité.

« *Professionnellement parlant, le fait de travailler dans les domaines de l'informatique et de la cybersécurité est très enrichissant car vous ne vous contentez plus de cocher des cases* », confesse Alan Maran. « *Cela va bien au-delà. Il faut savoir interpréter, mettre judicieusement son expertise technique à contribution, et c'est sur ces aspects que mon équipe en apprend le plus selon moi.* »

Conclusion

Une relation saine et solide entre les fonctions d'audit interne et de sécurité des systèmes d'information offre de nombreux avantages à l'organisation, à commencer par une meilleure compréhension et assimilation de son profil de cyber-risques (à la fois en termes de vulnérabilités, d'opportunités, de degré de maturité et de tests d'intrusion).

Une telle collaboration peut notamment contribuer à accroître la résilience et l'agilité de l'organisation face à d'éventuels cyberincidents, à des mutations ayant une incidence sur la cybersécurité ou encore à l'évolution du cadre réglementaire. Grâce à ce type de partenariat, la direction et le conseil d'administration bénéficient en outre d'une communication cohérente concernant les cyber-risques auxquels l'organisation est exposée, ainsi que ses besoins, ses priorités et son degré de maturité en matière de cybersécurité. Il est à noter que l'indépendance de l'audit interne peut être préservée, voire renforcée, dès lors que les deux équipes acquièrent une meilleure compréhension et une meilleure appréciation de leurs attributions, de leurs approches et de leurs responsabilités respectives. En nouant une relation durable, le responsable d'audit interne et le CISO peuvent concourir au renforcement de la cybersécurité de l'organisation, via la promotion d'une approche globale en la matière.

« *L'idée, c'est de passer d'une simple mission d'audit (qui consiste à tirer des observations pertinentes à partir d'une évaluation) à une véritable mobilisation pour la réussite de l'entreprise* », conclut Alan Maran.

3E PARTIE

Cyberincidents : comment les gérer et les surmonter ?

À propos des experts

Brian Tremblay

Brian Tremblay est responsable de l'activité Conformité chez Onapsis. Sa mission consiste à aider les clients à appréhender les défis et les opportunités nés de l'enchevêtrement accru des aspects de conformité, de cybersécurité et de continuité d'activité liés aux contrôles généraux informatiques et à la réglementation en vigueur (notamment la loi Sarbanes-Oxley (SOX) et le Règlement général sur la protection des données (RGPD)). Avant de rejoindre Onapsis, il était responsable de l'audit interne chez Acacia Communications, une entreprise spécialisée dans les semi-conducteurs de pointe. Il y a mis en place et piloté l'ensemble des activités d'audit interne et a contribué à l'établissement du dispositif de management des risques de l'entreprise (ERM) ainsi qu'à sa stratégie d'introduction en bourse (dont la mise en œuvre des exigences SOX). Avant cela, Brian Tremblay était directeur de l'audit interne chez Iron Mountain, où il était chargé de superviser l'ensemble des projets et des missions d'audit de la région Amérique du Nord et assurait un rôle d'interlocuteur auprès des responsables qualité mondiaux. Auparavant *senior manager* chez Houghton Mifflin Harcourt, il y a créé un service d'audit interne et mené à bien la mise en œuvre des exigences SOX. À ses débuts, il a travaillé chez Raytheon et chez Deloitte.

DaMon Ross Sr.

DaMon Ross Sr. a rejoint la société Cyber Defense International en 2020. Avec son équipe d'élite, il coordonne des opérations de cybersécurité et de veille des cybermenaces dans le but de proposer à un prix abordable des solutions et des services aux organisations qui n'ont pas les moyens de développer de tels outils en interne. Avant cela, DaMon Ross Sr. était directeur de l'activité Cybersécurité chez SunTrust Bank. Chargé de créer un centre d'intervention pour la cybersécurité opérationnel en continu, il y a mis en place des équipes spécialisées dans la cyberveille, dans la surveillance des cybermenaces, dans le traitement des cyberincidents et dans la cybercriminalité. En collaboration avec les services juridique, ressources humaines, sécurité interne, éthique et gestion des risques, il a mis en œuvre le tout premier programme de surveillance des menaces internes de la banque. Il a en outre contribué à la création de nombreux partenariats d'échange d'informations, notamment avec le Groupe de travail sur la cybercriminalité des Services secrets des États-Unis et le ministère américain de la Sécurité intérieure.

Introduction

Retour aux fondamentaux

Depuis maintenant longtemps, la cybersécurité est dans le viseur des organisations et de leur fonction d'audit interne, et l'année 2022 ne fait pas exception. En effet, les nouvelles propositions de la SEC relatives aux futures obligations de déclaration des organisations concernant leur stratégie et leur gouvernance en matière de cybersécurité, leur gestion des cyber-risques et leurs cyberincidents devraient, conjointement à d'autres projets de règles, donner encore un nouvel élan à cette thématique. Selon un rapport de l'Identity Theft Resource Center, 1 862 violations de données notoires ont été enregistrées en 2021 – un chiffre en hausse de 68 % par rapport à 2020, et qui va même jusqu'à battre le record historique de 2017 (1 506). Aucun secteur n'a été épargné[23].

Dans ce contexte, les organisations souhaitent – ou plutôt, exigent – des dispositifs de contrôle et des processus de cybersécurité clairs et robustes, qui reposent sur quelques fondamentaux : formation continue sur les risques et la réglementation y afférente, communication et consensus entre le conseil d'administration, la direction et l'audit interne. Pour rappel, la première partie de ce *Perspectives internationales* intitulé « La Cybersécurité en 2022 : état des lieux » aborde les répercussions potentielles des projets de règles en cours ; la deuxième partie expose quant à elle les avantages d'une relation symbiotique entre le responsable de l'audit interne et le responsable de la sécurité des systèmes d'information. Dans cette troisième et dernière partie, nous nous intéressons à l'élaboration et à la mise en œuvre d'une stratégie de gestion des cyberincidents, et plus précisément à la valeur ajoutée que peut apporter l'audit interne en évaluant les dispositifs de contrôle indispensables pour permettre à l'organisation de surmonter rapidement ce type d'incidents.

[23]. « Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises », Identity Theft Resource Center, 24 janvier 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

Les dispositifs de contrôle incontournables

Associer l'audit interne à la gestion des cyberincidents

Idées reçues en matière de gestion des cyberincidents

Bien que les expressions « plan de gestion des cyberincidents » et « plan de gestion et de reprise après incident de cybersécurité » aient une certaine précision et utilité, elles restent assez floues quant aux composantes desdits plans et aux conditions de leur efficacité.

Le rôle fondamental de l'audit interne consiste à fournir à l'organisation une assurance indépendante sur sa gestion des risques. Pour cela, il doit non seulement apporter une assurance concernant l'adéquation de la gestion des cyberincidents, mais aussi réaliser une évaluation appropriée des dispositifs de contrôle afin de vérifier que les risques et leurs effets sont maîtrisés, voire, mieux encore, évités. Or, pour ce faire, il ne s'agit pas uniquement d'observer la manière dont est traité le risque, quel qu'il soit. Il est plus efficace d'aborder la gestion des cyberincidents de manière cyclique et holistique, en misant sur des contrôles préventifs et des mesures d'intervention concrètes.

« *La gestion des risques forme une sorte de boucle* », explique Brian Tremblay, responsable de l'activité Conformité chez Onapsis, Inc. « *Au départ, les dispositifs de contrôle sont adéquats et les processus en place jugés efficaces. Puis, dès lors qu'un problème survient, nous évaluons si les dispositifs de contrôle ont fonctionné comme il se doit et si le scénario envisagé s'est déroulé comme prévu. À partir de là, nous identifions les modifications à apporter et le cycle recommence. Si vous vous contentez de n'intervenir qu'après coup, vous risquez de gaspiller votre temps et vos ressources. Le présent et l'avenir doivent être considérés sur un pied d'égalité, car l'entreprise d'aujourd'hui, c'est aussi l'entreprise de demain. Puisque les organisations semblent souvent avoir du mal avec ce concept, l'audit interne devrait tout particulièrement insister sur la question.* »

Des fondamentaux immuables

Certes, il est rare que les risques perdent en complexité et, compte tenu du degré de technicité élevé de la cybersécurité, l'appréhension des risques et l'identification des systèmes nécessaires pour les atténuer deviennent plus ardues à chaque nouvelle avancée technologique. Mais cela ne signifie pas pour autant que la structure fondamentale du plan de gestion des cyberincidents, et les dispositifs de contrôle qu'il intègre, changent du tout au tout.

Les dispositifs de contrôle en question, décrits dans les dernières lignes directrices complémentaires publiées par l'IIA, intitulées *Auditing Cyber Incident Response and Recovery*, répondent à quatre grands objectifs :

- **Élaborer un plan de gestion des incidents.** Il convient d'établir des politiques et des procédures précisant les modalités d'identification et de traitement des incidents. Élaboré avec le concours des principales parties prenantes, ce type de plan vise à définir les rôles et responsabilités de chacun. Il doit être testé dans le cadre d'une démarche de sensibilisation destinée à favoriser sa mise en œuvre.
- **Identifier les incidents.** Les processus d'analyse des données extraites des contrôles de détection permettent de déterminer l'existence d'un éventuel cyberincident, lequel déclenche la mise en œuvre d'un ou plusieurs plans de gestion.

- **Communiquer.** Les cyberincidents peuvent concerner de multiples acteurs. C'est pourquoi chaque plan de gestion doit intégrer une stratégie garantissant une communication adéquate et opportune des impacts identifiés et des mesures de résolution prises.
- **Identifier les mesures techniques de gestion et de résolution des incidents.** Les dispositifs de contrôle techniques à exécuter pour résoudre un incident et restaurer les systèmes dépendent en grande partie de la nature de l'incident en question. Ils nécessitent souvent une coordination des efforts en interne comme en externe[24].

La réalisation de ces objectifs et l'adoption d'un cadre de référence reconnu en matière de gestion des cyberincidents – tel que le Cadre pour le renforcement de la cybersécurité dans les infrastructures critiques du National Institute of Standards and Technology (NIST) – requièrent une expertise technique en termes de mise en œuvre, d'entretien et d'optimisation – expertise que possèdent les équipes informatiques et de la sécurité des systèmes d'information, et dont l'audit interne jouit aussi parfois. Certaines fonctions, moins techniques mais tout aussi essentielles, ont également la possibilité d'apporter une valeur ajoutée significative dans ce domaine. C'est notamment le cas de l'audit interne grâce, d'une part, à sa connaissance unique des différents services de l'organisation, et, d'autre part, à son indépendance, gage d'une assurance objective.

« *Du point de vue de l'audit interne, la stratégie de gestion des cyberincidents n'est pas différente de celle des autres risques car, ce qui compte réellement, c'est le processus en lui-même et le résultat qui en découle* », fait remarquer DaMon Ross Sr., fondateur de la société Cyber Defense International, LLC, et ancien directeur de l'activité Cybersécurité chez SunTrust Bank. « *Quel que soit le degré de technicité, n'importe quel auditeur interne habitué à travailler sur des processus sera à même d'identifier rapidement les points saillants.* »

Ce type de processus n'est pas sans rappeler ceux que l'audit interne peut être amené à rencontrer dans le cadre de missions portant sur le programme de conformité à la loi Sarbanes-Oxley (SOX), le plan de gestion de crise ou encore la stratégie de gestion des risques. « *Chaque organisation a beau avoir son propre jargon, un plan de gestion des cyberincidents reste fondamentalement une politique qui définit les caractéristiques d'un cyberincident, les rôles et responsabilités de chaque acteur concerné ainsi que les personnes décisionnaires* », constate DaMon Ross Sr.

Brian Tremblay partage cet avis. Il précise que les dispositifs de contrôle applicables aux cyber-risques se retrouvent également dans les cadres de référence utilisés aux fins de la gestion des risques associés à la conformité SOX.

Par exemple, les cybercriminels commencent généralement par pirater les droits d'accès nécessaires pour parvenir à leurs fins. Dans le panorama des risques, cela renvoie au risque d'accès non autorisé. Que l'on soit dans un contexte de conformité SOX ou de cyber-risque, cela ne change absolument rien selon Brian Tremblay. « *Réduits à leur plus simple expression, les risques, et, par extension, les dispositifs de contrôle associés, sont fondamentalement les mêmes.* »

Dispositifs de contrôle en matière de documentation

Comme l'a souligné Brian Tremblay, les dispositifs de contrôle se recoupent énormément d'un risque à l'autre. Citons par exemple l'importance d'un processus de documentation efficace. DaMon Ross Sr confirme que l'organisation doit s'attacher à comprendre l'imbrication des différentes actions visant à documenter les cyberincidents ainsi que les bonnes pratiques en la matière.

« *Il n'y a pas que les incidents de grande envergure qui comptent. Chaque organisation devrait avoir une fonction dédiée [à la documentation des cyberincidents]. Admettons qu'un ordinateur soit infecté par un logiciel malveillant. C'est*

[24]. *Auditing Cyber Incident Response and Recovery, Supplemental Guidance, Practice Guide*, The Institute of Internal Auditors, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf

précisément ce genre d'incident mineur qui peut dégénérer et, si le pire vient à se produire, une documentation adéquate peut aider à comprendre comment on en est arrivé là. Une fonction dédiée constitue un dispositif de contrôle en soi. »

Contrôles de détection et contrôles des infrastructures physiques

Autre type de contrôles clés associé au risque d'accès non autorisé : les contrôles des infrastructures physiques. Bien que l'on n'y songe pas d'emblée lorsqu'il est question de cybersécurité, une étude du Ponemon Institute publiée par IBM Security révèle tout de même que 10 % des attaques malveillantes enregistrées en 2020 résultent d'un accès non autorisé à des disques durs et à des serveurs contenant des informations sensibles, et que chacune de ces violations a coûté en moyenne 4,36 millions de dollars.

L'on entend par « infrastructures physiques » aussi bien des salles de serveurs sécurisées à accès restreint que des dispositifs de sécurité plus élémentaires tels que des portes verrouillées dans un bâtiment. Certes, protéger ces infrastructures est important. Mais il peut s'avérer encore plus utile de mettre en place des dispositifs de contrôle visant à détecter et à documenter les activités potentiellement suspectes.

« *Lorsque je parle d'infrastructures physiques, je ne parle pas de verrous, mais plutôt de la nécessité d'un processus visant à signaler et à documenter les activités qui génèrent véritablement un risque. Il ne s'agit pas de confondre l'entrée avec le plat de résistance* », ironise Brian Tremblay.

Pour DaMon Ross Sr, l'identification et l'assurance des systèmes concernés sont tout à fait du ressort de l'audit interne. Il précise : « *L'audit interne est à même d'identifier les systèmes les plus à risque ou les plus critiques pour la survie de l'organisation. Il est d'ailleurs fort probable qu'il les ait déjà recensés dans le cadre de missions d'assurance portant sur d'autres risques associés à la conformité aux lois et règlements fédéraux. Il lui suffit simplement d'élargir son analyse.* »

Alignement des attentes en matière de reprise après sinistre

Maintenir un processus de documentation efficace à toutes les étapes du plan de gestion des cyberincidents est primordial, tout comme le fait de communiquer les données qui en découlent et de s'assurer que les attentes en matière de détection des incidents et de reprise après sinistre sont alignées à l'échelle de l'organisation.

Selon Brian Tremblay, ce dernier point représente l'une des plus grosses lacunes des plans de gestion des cyberincidents, mais c'est aussi dans ce volet que l'audit interne peut apporter le plus de valeur ajoutée. « *L'audit interne a une double mission en matière de reprise après sinistre* », déclare-t-il. *La première : s'assurer que l'incident est réel et qu'il est possible de prouver son existence grâce à la documentation ou à un(e) quelconque processus ou technologie. La deuxième, dont j'ai pourtant rarement été témoin : s'entretenir avec l'ensemble des principaux acteurs [afin de définir] un délai réaliste de reprise après sinistre en fonction de l'appétence pour le risque de l'organisation.* »

Brian Tremblay précise que ce délai devra être déterminé par le responsable de l'application visée par l'incident (CISO, responsable de la chaîne, logistique, etc.). L'audit interne doit faire office d'intermédiaire entre ledit responsable et l'ensemble des parties qui utilisent l'application en question dans l'exercice de leurs missions quotidiennes.

« *Par exemple, le CISO peut considérer qu'un délai de 48 heures est raisonnable. Mais s'il n'en discute pas avec le directeur financier ou avec les autres responsables ou fonctions qui comptent sur le bon fonctionnement de la technologie concernée, il risque d'avoir des problèmes* », avertit Brian Tremblay. « *Le directeur financier peut par exemple approuver ce délai, à condition que ce ne soit pas la clôture des comptes. Dans le cas contraire, il n'acceptera aucune interruption, car l'organisation devrait alors demander une prolongation, ce qui ferait mauvais effet sur les marchés cotés.* »

Il ne doit pas nécessairement s'agir d'un rapport de force. L'idée, c'est plutôt que l'audit interne, par le dialogue, facilite l'atteinte d'un consensus qui concorde avec l'appétence pour le risque de l'organisation. Brian Tremblay s'explique : « *En cas de divergence d'opinions, [l'audit] interne peut par exemple s'enquérir du bien-fondé d'une telle prise de risque. Le*

directeur général peut alors arguer que la résolution du problème considéré coûterait extrêmement cher. Notre mission consiste à nous assurer que le plan [de reprise après sinistre] a été conçu en tenant compte de l'ensemble des parties prenantes concernées. »

Il poursuit : « *Je pense que notre profession n'est pas très douée dans ce domaine. Nous essayons tant bien que mal de cocher la case, en validant certains points, mais, lorsque nous procédons à l'examen des dispositifs de contrôle intégrés à un plan de reprise après sinistre, nous n'osons pas avouer de but en blanc avoir relevé une divergence d'attentes entre les différentes parties concernées par telle ou telle technologie. C'est pourtant un constat plus que valable, puisque nous avons identifié un risque jusqu'alors inconnu qui pèse lourdement sur l'organisation.* »

Un processus transversal

L'on pense souvent, à tort, que la responsabilité du plan de gestion des cyberincidents incombe en priorité au CISO et à l'équipe chargée de la sécurité. Mais ce n'est qu'en partie vrai. Sans doute possèdent-ils l'expérience et l'expertise nécessaires pour mettre en œuvre les aspects un peu plus techniques de la stratégie de cybersécurité. Néanmoins, il serait dangereux de présumer qu'ils ont la capacité – ou même la volonté – d'assumer seuls le poids de cette responsabilité.

« *La gestion des cyberincidents est – ou du moins devrait être – un processus transversal* », affirme DaMon Ross Sr. « *Pour moi, le temps de latence observé dans la réponse d'une organisation ne tient pas du tout à un quelconque manque d'expertise de la part du service informatique, mais plutôt à la difficulté à définir les rôles et les responsabilités des services dont la sécurité n'est pas l'obligation première. Ils ont d'autres chats à fouetter.* »

Pour DaMon Ross Sr, l'audit interne devrait impérativement s'attacher à corriger cette idée reçue et à promouvoir le partage des responsabilités entre l'ensemble des parties prenantes. « *Il ne s'agit pas tant de mettre l'accent sur l'équipe dédiée à la sécurité ni sur ses actions, mais plutôt d'attirer l'attention sur le soutien que les autres fonctions concernées de l'organisation peuvent lui apporter. Quand bien même cette équipe sait quoi faire, elle ne peut pas solliciter à l'excès l'aide des informaticiens et des développeurs back-end. Il y a toute un jeu politique à prendre en compte et, lorsque je me suis retrouvé dans cette situation, l'audit interne s'est avéré être un précieux partenaire. L'équipe sécurité ne peut pas lutter seule. Donc si l'on parvient à trouver un acteur relativement neutre pour identifier les lacunes dans le processus de l'organisation, ce sera bénéfique pour tout le monde.* »

Pour mettre en évidence les lacunes et clarifier les rôles, DaMon Ross Sr préconise que l'audit interne organise des exercices de simulation avec le concours d'un consultant externe. « *Dès lors que votre plan de gestion des cyberincidents est en place, il est possible de le tester. Un exercice de simulation consiste à réunir, physiquement ou virtuellement, le responsable des systèmes d'information, le responsable de la sécurité des systèmes d'information, les responsables de l'informatique, le directeur général et l'audit interne (c'est-à-dire tous les acteurs concernés), afin qu'ils explorent un scénario plausible. Même sans expertise technique, l'audit interne peut nourrir la discussion en se renseignant sur les responsabilités de chacun afin d'évaluer leur adéquation par rapport à la situation. Il pourrait très bien tenir le discours suivant : "À ce stade, votre équipe devrait en être aux étapes X et Y de notre plan, et, à dire vrai, elle pourrait même en être à l'étape Z." C'est précisément à ce moment-là que les masques tombent. La plupart des organisations doivent procéder à un exercice de simulation au moins une fois par an, mais je maintiens que l'audit interne devrait absolument s'en charger.* »

Conclusion

De la nécessité d'évoluer avec l'environnement des risques

Étant donné sa position unique au sein de l'organisation, l'audit interne mérite de pouvoir apporter sa contribution au plan de gestion des cyberincidents. Toutefois, cette reconnaissance ne doit pas le dispenser d'approfondir le sujet de la cybersécurité. En effet, à mesure que les infrastructures physiques vont faire place aux technologies basées sur le cloud, l'audit interne va inéluctablement devoir renforcer son expertise dans ce domaine.

« *Lorsque j'ai débuté ma carrière dans l'audit interne, ce qui m'a le plus attiré, c'était le caractère très généraliste du métier* », raconte Brian Tremblay. « *Vous découvrez et apprenez énormément de choses sans avoir besoin d'être un spécialiste. Mais l'univers de la technologie a tellement évolué que je commence sincèrement à me demander si les jours de l'auditeur interne généraliste ne sont pas comptés. À moins peut-être que la fonction d'audit interne devienne un jour experte de certains domaines fondamentalement essentiels pour l'organisation. Ainsi, au lieu d'avoir une équipe d'audit composée d'une dizaine d'auditeurs affectés aux opérations, à la conformité et aux états financiers, l'organisation comptera un auditeur spécialiste de la cybersécurité, un autre spécialiste des questions ESG, etc.* »

DaMon Ross Sr approuve. « *À un moment donné, au vu des technologies émergentes, comment voulez-vous appréhender pleinement les lacunes du processus de gestion des cyberincidents si vous n'avez pas le bagage adéquat ? C'est tout bonnement impossible.* »

Nous pouvons accomplir beaucoup avec les connaissances et les ressources à notre disposition, mais un avenir radicalement nouveau et prometteur se profile à l'horizon. Un avenir qui ne doit pas se faire sans l'audit interne.

Numéros précédents

Pour accéder aux numéros précédents des Perspectives internationales, visitez le site à l'adresse suivante : www.theiia.org/GPI.

Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse : globalperspectives@theiia.org.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'Institut des auditeurs internes (Institute of Internal Auditors, IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 215 000 membres et a délivré plus de 180 000 certifications CIA (Certified Internal Auditor) dans le monde. Plus d'informations sont disponibles sur le site www.theiia.org.

Avertissement

L'IIA publie ce document à titre informatif. Cette publication n'a pas vocation à apporter de réponses définitives à des situations spécifiques et est donc uniquement destinée à servir de guide. L'IIA recommande de consulter systématiquement des experts indépendants sur les points concernant des situations spécifiques. L'IIA décline toute responsabilité pour les cas où quiconque s'appuierait exclusivement sur cette publication.

Copyright

Copyright © 2022 de The Institute of Internal Auditors, Inc. Tous droits réservés. Prière d'adresser les demandes d'autorisation de reproduction à copyright@theiia.org.

Août 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101