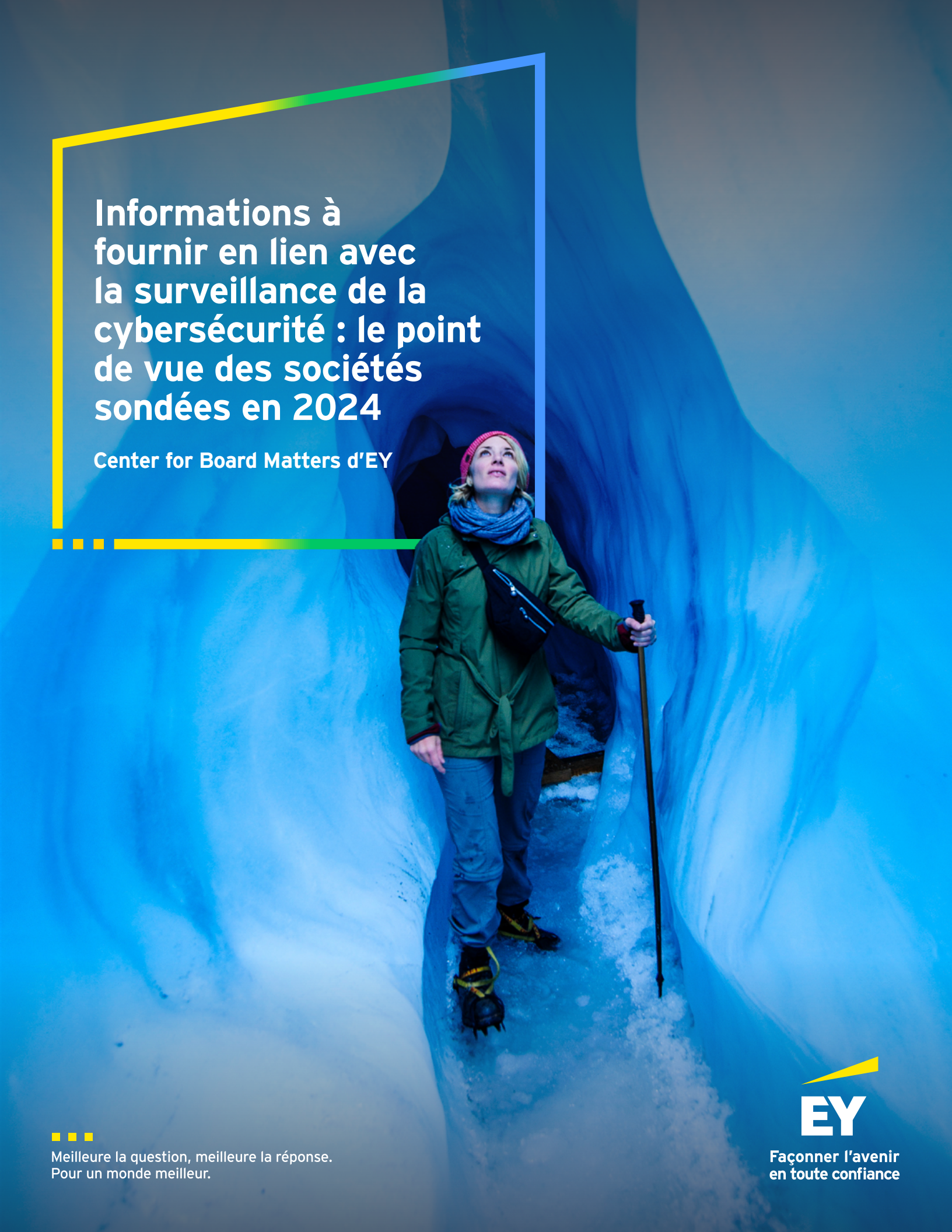
Informations à fournir en lien avec la surveillance de la cybersécurité : le point de vue des sociétés sondées en 2024

Center for Board Matters d'EY



Meilleure la question, meilleure la réponse.
Pour un monde meilleur.

EY
Façonner l'avenir en toute confiance

Alors que de nouvelles obligations d'information en matière de cybersécurité ont été approuvées par la SEC, de nombreuses sociétés fournissent volontairement de plus en plus d'informations aux investisseurs sur leurs activités de surveillance de la cybersécurité.

L'exercice en est souvent un d'équilibre, car les sociétés cherchent à fournir à la communauté des investisseurs des informations pertinentes sur l'atténuation des risques et les mesures qu'elles prennent pour répondre aux incidents importants, tout en limitant la diffusion d'informations susceptibles d'être exploitées par des adversaires ou des personnes malintentionnées.

La présentation d'informations joue un rôle important dans la communication avec les investisseurs et les parties prenantes en général. Plus de 25 années se sont écoulées depuis que les conseils inscrivent le cyberrisque à l'ordre du jour de leurs réunions, et les administrateurs comprennent désormais qu'il s'agit d'un enjeu en constante évolution dont la surveillance efficace requiert une diligence de tous les instants et une approche ciblée. Au cours de la dernière année, les cybermenaces se sont grandement complexifiées, ce qui a non seulement incité les entreprises à améliorer leurs cadres de cybersécurité, mais également amené leurs adversaires à perfectionner leurs attaques.

Évolution importante des risques pour la cybersécurité

Les nouvelles technologies donnent naissance à des menaces grandissantes

La quasi-totalité des sociétés (93 %) utilise désormais l'intelligence artificielle (IA) générative d'une façon ou d'une autre, et elles sont nombreuses à prévoir de l'utiliser comme moyen d'améliorer la cybersécurité[1], et plus précisément de relever les cyberrisques potentiels, de détecter les vulnérabilités et les brèches de sécurité, et de prioriser les efforts de cybersécurité. Toutefois, les cybermenaces continuent de prendre de l'ampleur. L'an dernier, le FBI a constaté une hausse de 10 % des plaintes et de 22 % des pertes subies, qui s'élèvent maintenant à 12,5 milliards de dollars par année[2]. Dans près d'un tiers (32 %) de ces incidents, les attaquants ont eu recours à un stratagème d'extorsion, comme un rançongiciel[3].

La plupart des brèches de sécurité informatique sont en partie attribuables aux employés

Dans plus des deux tiers des cas d'intrusion informatique, des employés sont en partie responsables, ayant cédé à de l'hameçonnage, à de la manipulation psychologique ou à d'autres méthodes employées contre eux pour obtenir leurs identifiants et les exploiter.

Les cyberrisques émanant de tiers sont en progression

La dépendance envers des tiers pour le maintien d'environnements d'exploitation informatiques de plus en plus complexes accroît la surface d'exposition aux menaces, c'est-à-dire l'ensemble des points exposés qu'un attaquant pourrait exploiter. Elle peut également créer des points faibles dans des systèmes critiques, qui peuvent alors être perturbés.

Le recours à des conseillers externes est de plus en plus courant

La cybersécurité étant, par nature, en constante évolution, elle requiert de la part des administrateurs et conseils une diligence de tous les instants. La proportion de sociétés qui ont fourni des informations sur le recours à des conseillers externes indépendants a plus que doublé, passant de 43 % en 2023 à 87 % en 2024, et 10 % d'entre elles ont indiqué que leur conseil était en communication avec un tel conseiller.

1. *State of Security 2024: The Race to Harness AI, Splunk.*
2. *2023 Internet Crime Report, Federal Bureau of Investigation (FBI), Internet Crime Complaint Center.*
3. *We've seen the data on how they're getting in, Verizon business, 2024.*
4. *« Technical Line: A closer look at the SEC's new rules on cybersecurity disclosures », EY, 19 septembre 2024.*

Tendances en matière d'informations sur la cybersécurité observées en 2024

Depuis que nous avons commencé à suivre les informations fournies sur la cybersécurité en 2018, la quantité d'informations publiées de façon volontaire a augmenté de manière constante. La SEC impose maintenant aux sociétés cotées en Bourse la présentation d'un large éventail d'informations sur la gestion et la surveillance des risques liés à la cybersécurité, y compris sur la façon dont le conseil encadre les cyberrisques[4].

Dans l'ensemble, les sociétés ouvertes publient de plus en plus d'informations sur la cybersécurité. Chacun des aspects de la cybersécurité que nous suivons dans les informations fournies a pris de l'ampleur depuis que nous avons lancé ce projet en 2018. L'analyse des informations sur la surveillance de la cybersécurité fournies par les sociétés figurant au palmarès Fortune 100 nous permet de dresser les constats suivants :

- Les comités d'audit continuent d'assurer la surveillance de la cybersécurité. Selon 81 % des sociétés du palmarès Fortune 100 sondées, malgré sa charge de travail croissante, le comité d'audit demeure responsable de la surveillance de la cybersécurité, une proportion en hausse par rapport à 61 % en 2018.
- Les compétences en cybersécurité sont recherchées. Bien qu'aux termes de la règle de la SEC sur les informations à fournir en lien avec la cybersécurité, les sociétés ne soient pas tenues d'indiquer quelles compétences les membres de leur conseil possèdent dans ce domaine, notre examen de leurs documents révèle que de telles compétences sont recherchées. Près des trois quarts (72 %) des sociétés indiquent que l'informatique est un domaine d'expertise recherché au sein du conseil et presque autant de sociétés (71 %) mentionnent la cybersécurité dans au moins une de leurs biographies d'administrateur, contre 34 % en 2018.
- Des spécialistes des cyberrisques collaborent avec le conseil. Quelque 70 % des sociétés – contre seulement 9 % en 2018 – indiquent que le chef de la sécurité de l'information présente au conseil des informations sur les cyberrisques.
- Les conseils consacrent du temps à la cybersécurité. Plus de la moitié (57 %) des sociétés ont indiqué que leur conseil et la direction se réunissaient au moins une fois l'an ou chaque trimestre pour aborder des questions de cybersécurité. Les autres sociétés demeurent plus vagues, mentionnant que de telles réunions sont fréquentes ou périodiques. Ces mentions sont au moins quatre fois plus nombreuses qu'en 2018.
- Les exercices de préparation sont monnaie courante. Près de la moitié des sociétés (47 %), comparativement à seulement 3 % en 2018, déclarent à présent effectuer, dans le cadre de leurs efforts de préparation, des exercices de simulation ou des tests sur le degré de préparation à l'intervention

Vous trouverez ci-après une analyse des informations fournies par les sociétés du palmarès Fortune 100. Au 31 mai 2024, 79 d'entre elles avaient déposé leur circulaire d'information et leur formulaire 10-K; il s'agit donc du bassin de sociétés sondées aux fins de cette analyse. Celle-ci est le reflet d'observations formulées à partir des documents déposés par ces sociétés au cours des sept dernières années. Étant donné la période à laquelle correspondent certains exercices, le taux de présentation des informations sur la cybersécurité dont la fourniture est désormais obligatoire peut être inférieur à 100 %. Dans le cas de l'information facultative, le fait qu'une société n'ait pas mentionné une activité ne signifie pas forcément qu'elle ne l'exerce pas. Cela signifie simplement qu'elle n'a pas fourni d'informations à ce sujet dans ses documents.

Informations sur la cybersécurité fournies par les sociétés du palmarès Fortune 100 de 2018 à 2024

Catégorie d'activités de surveillance par le conseil	Sujet	2024	2022	2020	2018
Surveillance par un comité du conseil*	Sociétés ayant indiqué qu'au moins un comité du conseil était responsable de la surveillance des questions de cybersécurité*	95 %	89 %	85 %	76 %
	Sociétés ayant indiqué que la surveillance des questions de cybersécurité relevait du comité d'audit	81 %	72 %	67 %	61 %
	Sociétés ayant indiqué que la surveillance relevait d'un comité responsable de questions autres que d'audit (p. ex., gestion des risques, technologie)	29 %	28 %	24 %	19 %
	Sociétés ayant indiqué que la surveillance relevait d'un comité de gestion des risques	13 %	11 %	10 %	9 %
	Sociétés ayant indiqué que la surveillance relevait d'un comité de la technologie	10 %	9 %	8 %	9 %
	Sociétés ayant indiqué que la surveillance relevait d'un autre comité (p. ex., comité de conformité)	8 %	8 %	8 %	3 %
Compétences et expérience des administrateurs	La cybersécurité est présentée comme un domaine d'expertise recherché pour le conseil ou est mentionnée dans la biographie d'au moins un administrateur	85 %	68 %	61 %	42 %
	La cybersécurité est présentée comme un domaine d'expertise recherché pour le conseil	72 %	51 %	35 %	19 %
	La cybersécurité est mentionnée dans la biographie d'au moins un administrateur	71 %	56 %	49 %	34 %
Rapports de la direction au conseil	Informations concernant les rapports que la direction présente au conseil et/ou au(x) comité(s) surveillant les questions de cybersécurité**	96 %	78 %	57 %	51 %
	Mention d'au moins un dirigeant responsable de fournir des informations sur la cybersécurité au conseil (p. ex., chef de la sécurité de l'information ou chef de l'information)	84 %	42 %	25 %	18 %
	Mention du chef de la sécurité de l'information en particulier	70 %	28 %	16 %	9 %
	Mention du chef de l'information en particulier	28 %	16 %	10 %	8 %
	Mention du chef de la technologie en particulier	11 %	4 %	0 %	8 %
	Formulations concernant la fréquence des rapports de la direction au conseil ou au comité (la plupart de ces formulations n'étaient pas précises)	95 %	70 %	46 %	34 %
	Mention du fait que les rapports sont présentés au moins annuellement ou chaque trimestre; les autres sociétés ayant utilisé des termes comme « régulièrement » ou « périodiquement »	57 %	44 %	18 %	13 %
Préparation à l'intervention	Mention des mesures prises pour réduire les risques liés à la cybersécurité, comme la mise en place de processus, de procédures et de systèmes	100 %	99 %	95 %	85 %
	Mention de l'adoption d'un cadre ou d'une norme externe**	57 %	20 %	4 %	2 %
	National Institute of Standards and Technology (NIST)	47 %	14 %	3 %	1 %
	Organisation internationale de normalisation (ISO)	20 %	4 %	1 %	1 %
	Autre**	14 %	6 %	0 %	0 %
	Mentions relatives à l'état de préparation à l'intervention, comme la planification, la reprise après sinistre ou la continuité des activités	95 %	73 %	65 %	53 %
	Mention de mesures de préparation comprenant des exercices de simulation ou des tests sur le degré de préparation à l'intervention	47 %	9 %	6 %	3 %
	Mention du fait que la société maintient un certain niveau d'assurance cybersécurité	25 %	20 %	13 %	8 %
	Inclusion de la cybersécurité dans la rémunération de la haute direction	11 %	10 %	6 %	1 %
Sensibilisation et formation	Mention de l'utilisation d'activités de sensibilisation et de formation pour réduire les risques liés à la cybersécurité	82 %	47 %	28 %	15 %
Collaboration avec des intervenants externes en matière de sécurité	Mention de collaboration avec des pairs, des groupes sectoriels et des décideurs politiques	28 %	14 %	10 %	6 %
Recours à des conseillers externes	Mention du recours à un conseiller externe indépendant	87 %	34 %	16 %	15 %

Les pourcentages tiennent compte de l'ensemble des informations fournies par les sociétés. Les données proviennent de 79 sociétés qui figuraient au palmarès Fortune 100 de 2024 et qui avaient déposé, au 31 mai 2024, un formulaire 10-K et une circulaire d'information pour l'exercice considéré.

** Certaines sociétés confient la surveillance de la cybersécurité à plus d'un comité du conseil d'administration.*

*** Certaines sociétés indiquent qu'elles cherchent à se conformer à plus d'un cadre ou d'une norme externe. Ces cadres normatifs ont divers champs d'application et peuvent ne pas régir tous les aspects de la société à la fois; certains d'entre eux, mais pas tous, comprennent un mécanisme de certification ou d'attestation externe. Les autres cadres normatifs qui ne sont pas expressément mentionnés dans les présentes comprennent, entre autres, les normes de sécurité des données de l'industrie des cartes de paiement, la Health Information Trust Alliance, et les contrôles 1 et 2 au niveau du système et au niveau organisationnel.*

Comité chargé de la surveillance

En 2018, environ trois sociétés sur quatre (76 %) faisaient mention d'au moins un comité responsable de la surveillance des cyberrisques, contre 96 % aujourd'hui. Comme par le passé, 81 % des sociétés indiquent que le comité d'audit est responsable de la surveillance de la cybersécurité. Seulement 13 % des sociétés sondées indiquent qu'elles ont créé un comité de gestion des risques autonome – il s'agit, dans bien des cas, de sociétés du secteur des services financiers, dans lequel la constitution d'un tel comité du conseil peut répondre à une exigence réglementaire. Un nombre encore plus faible de sociétés a confié la surveillance des cyberrisques à un comité responsable de la technologie (10 %) ou à un comité chargé d'autres questions (8 %), comme la conformité.

Les technologies émergentes devraient transformer les modèles d'affaires dans les années à venir, et bon nombre d'entre elles, comme l'IA générative, auront une incidence sur la cybersécurité. De plus, le perfectionnement croissant des méthodes d'hameçonnage et de piratage psychologique employées pour perpétrer des attaques pourrait amener les conseils à se pencher sur des sujets qui ne sont traditionnellement pas abordés dans les discussions sur les menaces et les mesures à prendre pour les contrer. Des sujets tels que la culture de la cybersécurité et l'appétit pour les cyberrisques pourraient devoir être examinés plus sérieusement.

Questions que le conseil devrait se poser

- Comment le conseil s'y prend-il pour aligner le mieux possible les responsabilités de ses comités et les siennes afin de surveiller adéquatement l'évolution des besoins de la société en matière de cybersécurité?
- Le comité auquel incombe la surveillance des cyberrisques dispose-t-il du temps et des ressources nécessaires pour bien faire son travail?
- Quelles informations la direction a-t-elle communiquées au conseil pour l'aider à déterminer quels actifs et partenaires commerciaux clés, y compris les tiers et les fournisseurs, sont les plus vulnérables en cas de cyberattaques?

Compétences et expérience des administrateurs

Puisque les cybermenaces et la cyberdéfense sont en constante évolution, les conseils d'administration cherchent sans cesse à améliorer leurs compétences et à accroître leur expertise. Cette année, 72 % des sociétés ont mentionné la cybersécurité comme domaine d'expertise recherché pour le conseil d'administration. Un tiers des sociétés a indiqué qu'au moins un administrateur avait auparavant acquis de l'expérience dans un poste de chef de la sécurité de l'information, de chef de l'information ou de chef de la technologie. Seulement 29 % des sociétés ont cependant déclaré que les membres du conseil avaient pris part à des activités de formation sur la cybersécurité.

Les conseils peuvent prendre divers moyens pour rehausser leur expertise en cybersécurité. Certains cherchent à s'adjoindre un spécialiste qui possède une expérience approfondie et pertinente de la cybersécurité et qui en connaît les derniers développements. D'autres se concentrent plutôt sur le perfectionnement des compétences de leurs membres, et pour ce faire organisent des séances d'information auxquelles des spécialistes internes ou externes sont invités ou participent à des conférences ou à des programmes de formation certifiés, et créent des comités consultatifs, officiels ou non, qui demeurent en tout temps à la disposition du conseil d'administration de la société ou de ses comités.

Questions que le conseil devrait se poser

- Dans quelle mesure les compétences et l'expertise actuelles des membres du conseil répondent-elles aux besoins actuels et futurs de la société?
- Lorsque le conseil doit s'appuyer sur des connaissances spécialisées, comment les obtient-il?
- Que pense le conseil de l'importance de s'adjoindre un unique spécialiste de la cybersécurité ou d'accueillir divers membres possédant une expertise en cybersécurité?

Relations entre le conseil et la direction

Cette année encore, nous avons constaté qu'un nombre croissant de sociétés précisaient, dans leurs documents, que le chef de la sécurité de l'information fournit des informations au conseil (70 % cette année, contre seulement 9 % en 2018). En 2018, 8 % des sociétés avaient indiqué que la personne directement responsable de la cybersécurité était le chef de l'information, et un autre 8 %, que cette personne était le chef de la technologie. En 2024, ces proportions sont plus élevées, s'établissant respectivement à 28 % et à 11 %. Quelque 57 % des sociétés sondées ont indiqué que ces interactions avaient lieu au moins annuellement ou trimestriellement, tandis que les autres sociétés ont simplement mentionné que les rencontres étaient fréquentes, les qualifiant de « régulières » ou de « périodiques ».

Questions que le conseil devrait se poser

- Comment le conseil fait-il pour s'assurer de recevoir les bonnes informations sur les cyberrisques de la part de la direction?
- Comment le conseil fait-il pour s'assurer que les informations sur les cyberrisques qu'il reçoit proviennent des bonnes personnes?
- La direction a-t-elle une vision globale des cyberrisques, qui tient compte à la fois des menaces, des mesures d'intervention à mettre en place et de l'état de la culture de la cybersécurité de la société?

Préparation à l'intervention en cas d'incidents et recours à des conseillers externes

Parce qu'il est fort probable, voire certain, qu'un incident de sécurité informatique se produira, il est absolument crucial de s'y préparer. En 2018, une seule et unique société avait mentionné l'adoption d'un cadre ou d'une norme externe en matière de cybersécurité. Les choses ont bien changé. Cette année, 47 % des sociétés ont indiqué qu'elles appliquaient le cadre de la National Institute of Standards and Technology (NIST), et 20 % des sociétés, les normes ISO. Près de la moitié des sociétés (47 %) déclarent en outre effectuer des exercices de simulation ou des tests sur le degré de préparation à l'intervention. De telles activités ont acquis une popularité considérable, les informations fournies à leur sujet étant 3,5 fois plus nombreuses qu'elles ne l'étaient dans le précédent cycle de présentation de l'information. Même si les caractéristiques d'une simulation ne peuvent correspondre en tous points à celles d'une situation réelle, l'exercice peut tout de même servir à tester la résistance des processus et procédures internes et à développer les bons réflexes en prévision d'une grave défaillance.

Un nombre de plus en plus grand de sociétés déclare faire appel à des conseillers externes indépendants pour se préparer à intervenir en cas d'incident et mieux comprendre le contexte dynamique de la cybersécurité. De fait, cette année, 87 % des sociétés ont mentionné qu'elles recouraient aux services d'un conseiller externe indépendant, un nombre deux fois plus élevé que l'an dernier, et 10 % des sociétés sondées ont indiqué que leurs administrateurs étaient en communication avec un tel conseiller.

Questions que le conseil devrait se poser

- Quel cadre externe de cybersécurité la société applique-t-elle? Pourquoi la direction l'a-t-elle choisi et, si c'était à refaire, prendrait-elle la même décision aujourd'hui?
- Comment le conseil fait-il pour s'assurer que les plans d'intervention de la société en cas de crise liée à la cybersécurité sont à jour et pertinents?
- Quels sont les rôles et responsabilités du conseil en cas d'incident de sécurité informatique? Quelles sont les responsabilités de la direction en pareil cas?

Pratiques de pointe en surveillance de la cybersécurité

À la lumière des discussions qu'EY a menées avec des administrateurs, des groupes sectoriels, des leaders en cybersécurité et des professionnels en matière de politiques publiques, nous avons recensé ces 10 pratiques de pointe pour aider les conseils dans leur surveillance des cyberrisques.

Pratique	Mesures à prendre	Questions à se poser
Élever le ton	Considérer la cybersécurité comme une préoccupation majeure dans toutes les discussions du conseil. Si la technologie est la pierre angulaire de la plupart des décisions d'affaires, les questions liées au cyberrisque devraient par conséquent faire partie des discussions du conseil et de la direction portant sur la stratégie, les plans de croissance des produits et des services, la transformation numérique, etc.	▪ Quels secteurs de notre entreprise sont les plus vulnérables aux perturbations de la cybersécurité? ▪ Quelles sont les vulnérabilités qui représentent des risques existentiels pour la société?
Rester alerte	Aborder les nouvelles difficultés et menaces découlant du télétravail et de l'expansion de la transformation numérique.	▪ Comment la société évalue-t-elle, surveille-t-elle et améliore-t-elle sa culture en matière de cyberrisques? ▪ Quelle personne est la mieux placée pour fournir cette information au conseil?
Déterminer la valeur à risque	Faire le rapprochement entre la valeur à risque en dollars et la tolérance au risque du conseil, y compris l'efficacité de la couverture de cyberassurance.	▪ Quels indicateurs montrent le mieux la valeur qui est à risque pour la société? ▪ La tolérance au risque de la société convient-elle à la valeur à risque de la société?
Tirer parti des nouveaux outils analytiques	Pareils outils informent le conseil d'administration des cyberrisques – des incidents très probables dont l'incidence est faible aux incidents peu probables dont l'incidence est élevée (comme un événement de type cygne noir).	▪ Comment la direction détermine-t-elle quels risques doivent figurer à l'ordre du jour du conseil? ▪ Dans quelle mesure le conseil a-t-il la certitude qu'il tient des discussions sur les risques à cibler?
Intégrer la sécurité dès le début	Adopter une philosophie axée sur la « sécurité dès la conception » pour la mise au point de nouvelles technologies et de nouveaux produits et arrangements commerciaux. L'an dernier, la Cybersecurity and Infrastructure Security Agency (CISA), le Federal Bureau of Investigation (FBI), la National Security Agency (NSA) et des partenaires internationaux ont publié des principes et des approches de la sécurité dès la conception.	▪ Quelle est l'approche de la société à l'égard de la sécurité dès la conception? ▪ Comment le conseil peut-il s'assurer que cette approche est suivie?
Évaluer de manière indépendante	Obtenir une évaluation rigoureuse par un tiers du programme de gestion des cyberrisques de la société, y compris des tests des systèmes et des processus essentiels.	▪ Comment la direction a-t-elle déterminé vers qui se tourner pour une obtenir une évaluation par un tiers? ▪ Quels sont les principaux points de désaccord avec l'examen par un tiers et quelles sont les mesures prévues?
Évaluer le risque lié aux tiers	Comprendre les processus de la direction permettant de cerner, d'évaluer et de surveiller le risque lié aux fournisseurs de services et aux parties à la chaîne d'approvisionnement de la société.	▪ Quels tiers représentent un point de défaillance unique pour les systèmes critiques? ▪ Que savons-nous des risques posés par les tiers et leurs fournisseurs et prestataires de services en aval?
Mettre à l'essai les plans d'intervention et de reprise	Renforcer la résilience de l'entreprise en réalisant des simulations rigoureuses et en établissant des protocoles en collaboration avec des spécialistes indépendants avant une crise.	▪ Quelle expérience le conseil possède-t-il des exercices de simulation réalistes et complexes? ▪ De quelle façon les résultats des simulations sont-ils intégrés au plan d'intervention en cas de crise de la société?
Comprendre les protocoles d'escalade des incidents	Disposer d'un plan de communication défini qui précise le moment auquel il convient d'informer le conseil des incidents, notamment des attaques par rançongiciel.	▪ Dans quelles circonstances le conseil est-il avisé et après combien de temps? ▪ Quel rôle le conseil joue-t-il dans le plan et comment sera-t-il informé si son rôle change?
Suivre les nouveautés en matière de réglementation et de politiques publiques	Rester au fait de l'évolution des pratiques de surveillance, des obligations d'information, des structures d'information et des mesures, et en comprendre aussi l'incidence sur la conformité réglementaire de la société.	▪ Qui est responsable de suivre les nouveautés en matière de réglementation et de politique publique? ▪ Comment les groupes pertinents sont-ils avisés et les processus mis à jour avec les changements pertinents?

Cybersécurité – Nouveautés en matière de politique publique

Au cours de la dernière année, tandis que les assemblées législatives des États étaient très actives dans le domaine de la cybersécurité, aucun texte législatif définitif n'a été adopté au niveau fédéral, et un nombre relativement restreint de modifications a été apporté à des textes réglementaires. Voici certains des faits nouveaux qui pourraient avoir une incidence sur les conseils d'administration et les sociétés.

Au niveau fédéral, les organismes de réglementation ont fait progresser les politiques relatives à la cybersécurité sur plusieurs fronts. En ce qui concerne les sociétés du secteur des infrastructures essentielles, la Cybersecurity and Infrastructure Security Agency (CISA) a publié un avis de projet de réglementation aux fins de mise en œuvre de la loi intitulée *Cyber Incident Reporting for Critical Infrastructure Act*. Cette loi impose aux sociétés du secteur l'obligation de fournir des informations sur les cyberincidents, qui comprennent les sommes versées dans le cadre d'attaques par rançongiciel. On s'attend à ce que la CISA publie pour consultation une nouvelle version de son projet de réglementation.

La Federal Communications Commission (FCC) a lancé un programme appelé Cyber Trust Mark. Il s'agit d'un programme d'étiquetage volontaire en matière de cybersécurité qui vise à fournir aux consommateurs des informations claires sur la sécurité de leurs appareils connectés à Internet et à les aider de ce fait à prendre des décisions d'achat éclairées. De façon semblable à « Energy Star », initiative administrée par l'Environmental Protection Agency, le programme permettra l'étiquetage des appareils connectés à Internet qui répondent aux critères de cybersécurité de la FCC. Celle-ci a d'ailleurs publié un projet de règlement pour la mise en œuvre du programme en juillet 2024, dont le lancement pourrait avoir lieu vers la fin de l'année.

SEC

Le président de la SEC, Gary Gensler, continue de mettre les parties prenantes en garde contre les risques liés à la cybersécurité. En juin 2024, il a entre autres déclaré que les cybermenaces représentaient un danger de plus en plus sérieux tant pour l'organisme que les marchés.

Le personnel de la SEC a publié diverses directives se rapportant à la règle sur les informations à fournir en lien avec la cybersécurité. Il s'agit notamment de directives qui visent à indiquer aux sociétés ouvertes comment signaler les incidents de sécurité informatique selon leurs différents degrés d'importance. D'autres directives adressées aux émetteurs mettent l'accent sur la nécessité, pour les sociétés, d'évaluer et de signaler les brèches de sécurité informatique importantes associées à des demandes de rançons, et ce, même lorsqu'elles semblent avoir été réglées par le versement de telles rançons.

La SEC a aussi adopté, en mai 2024, des modifications du Règlement S-P selon lesquelles les courtiers, les sociétés de placement et d'autres acteurs du secteur des valeurs mobilières doivent mettre en œuvre d'un plan d'intervention aux fins de détection et de gestion des possibles atteintes à l'intégrité des données. Ces entités sont également tenues d'informer sans délai les personnes dont les informations sensibles pourraient avoir été compromises ou être raisonnablement exposées à un risque d'accès ou d'utilisation non autorisés.

La SEC continue de prendre des mesures coercitives contre les sociétés en situation de défaut liée à la cybersécurité. Selon son rapport sur les résultats de leur mise en application pour l'exercice 2023, la SEC a sanctionné des sociétés qui ont fait des déclarations trompeuses sur la protection des données de clients et fourni des informations insuffisantes sur des attaques par rançongiciel d'envergure qui ont touché des milliers de personnes. Plus récemment, l'organisme a sévi contre des sociétés qui, entre autres manquements, avaient omis de protéger les titres et les fonds de leurs clients, avaient minimisé les risques liés à la cybersécurité et n'avaient pas signalé des intrusions informatiques.

Travaux des assemblées législatives étatiques

En 2024, les assemblées législatives des États ont déposé 132 projets de loi relatifs à la cybersécurité et en ont étudié 250 (nombre qui comprend des projets dont l'étude avait été amorcée en 2023). Sont entrées en vigueur 27 lois qui prévoient notamment des mesures visant à obliger les assureurs à enquêter sur les incidents liés à la sécurité informatique et à en informer le commissaire aux assurances, ainsi qu'à protéger les systèmes électoraux et les réseaux électroniques, à prévoir des mesures de sécurité dans les marchés publics, et à financer la formation et l'éducation dans le domaine de la cybersécurité. Des lois ont été promulguées en Alaska, en Arizona, en Californie, en Floride, en Indiana, en Iowa, au Kansas, en Louisiane, au Maryland, au Massachusetts, au Minnesota, au Mississippi, dans l'État de New York, en Ohio, en Oklahoma, en Pennsylvanie, au Rhode Island, au Dakota du Sud, au Tennessee, en Utah, en Virginie, dans l'État de Washington et en Virginie-Occidentale.

Points à retenir sur la surveillance par les conseils

Les administrateurs et les conseils doivent comprendre les mesures d'atténuation des cyberrisques et les concepts clés qui s'y rattachent pour pouvoir surveiller efficacement les possibilités et défis que peuvent représenter les technologies, nouvelles ou non. Les conseils qui se démarquent priorisent la surveillance de la cybersécurité et, pour ce faire, en tiennent compte dans toutes les discussions qui s'y prêtent, échangent avec une diversité de membres de la direction et de spécialistes externes, s'assurent de posséder les compétences requises ou d'y avoir accès, et mènent des exercices d'intervention et en tirent des leçons, qu'ils intègrent ensuite aux façons de faire de la société. Ils demeurent aussi au fait de la réglementation et de son évolution et tendent à fournir de façon sans cesse plus transparente et opportune des informations sur les moyens que prend la société pour identifier et traiter les principaux risques liés à la cybersécurité.

Exemples de libellés sur la cybersécurité pour les sociétés ouvertes

Chartes

Les chartes des comités du conseil doivent représenter fidèlement les responsabilités du comité en question et doivent être mises à jour au besoin. Les chartes du comité de la technologie de Citigroup Inc. et du comité de la technologie d'Humana Inc. illustrent toutes deux très bien en quoi peuvent consister les responsabilités dévolues aux comités chargés de la gouvernance des cyberrisques.

Mettre en évidence les compétences du conseil en matière de cybersécurité

La publication d'une grille de compétences et de biographies d'administrateurs dans la circulaire d'information annuelle est une pratique de pointe pour les sociétés qui fournissent des informations sur l'expertise de leur conseil. Ces deux méthodes ont été employées, par exemple, dans la circulaire d'information de 2024 de Lockheed Martin (pages 29 à 37). La grille qu'on y trouve présente les compétences et l'expérience générales des administrateurs, et chaque compétence y est définie clairement. Elles sont ensuite énumérées dans chacune des biographies des administrateurs.

Informations sur la surveillance des cyberrisques exercée par le conseil, y compris la façon dont il s'y prend pour se tenir informé et dont le conseil ou un comité du conseil aborde le risque dans le cadre de sa surveillance de la stratégie d'affaires, de la gestion des risques et des questions financières

Les risques liés à la cybersécurité sont surveillés par des comités de gestion, qui rendent compte au comité de gestion des risques de la société, puis au comité de l'exploitation et de la technologie ainsi qu'au conseil d'administration. Le comité de l'exploitation et de la technologie est le premier responsable de la surveillance des risques liés aux activités, aux technologies et à l'exploitation, ce qui comprend les questions relatives à la sécurité de l'information, la fraude, la protection et la confidentialité des données, la continuité des activités et la résilience de l'entreprise, et les cyberrisques (y compris la revue de ces derniers et des méthodes employées pour les gérer). Conformément à sa charte, le comité de l'exploitation et de la technologie reçoit tous les trimestres, de la part des cadres supérieurs du service des technologies, du service de l'exploitation et du service de la gestion des risques non financiers, des rapports sur les risques auxquels sont exposées les activités de la société et les mesures que la direction a prises pour surveiller et maîtriser pareilles expositions. Ces rapports comprennent des informations à jour sur le programme de cybersécurité de la société, les menaces présentes dans son environnement externe et les programmes qu'elle a mis en place pour traiter et atténuer les risques liés à l'évolution des menaces informatiques.

Le comité de l'exploitation et de la technologie reçoit aussi annuellement, de la part d'une partie externe, une évaluation indépendante des principaux aspects du programme de cybersécurité de la société, et tient des réunions conjointes avec le comité d'audit et le comité de gestion des risques, au besoin. Le conseil d'administration ou le comité de l'exploitation et de la technologie passe en revue et approuve, au moins tous les ans, la politique sur le programme mondial de cybersécurité, la politique mondiale sur la sécurité de l'information et la politique mondiale sur les technologies. Le président du comité de l'exploitation et de la technologie rend régulièrement compte des risques liés à la cybersécurité et d'autres questions dont il est chargé de la revue au conseil d'administration. En outre, des présentations distinctes à propos des risques liés à la cybersécurité sont faites au conseil d'administration, et, conformément aux politiques de gouvernance de l'entreprise, tous les administrateurs sont invités à assister aux réunions du comité de l'exploitation et de la technologie et ont accès aux documents distribués pendant la réunion.

La haute direction, y compris les cadres supérieurs mentionnés précédemment, s'entretient des faits nouveaux en matière de cybersécurité avec le président du comité de l'exploitation et de la technologie à tout moment entre les réunions du conseil, au besoin. Le comité de l'exploitation et de la technologie se réunit régulièrement avec la direction, y compris le responsable de la gestion des risques non financiers, et les cadres supérieurs du service des technologies et du service de l'exploitation.

Préparation à l'intervention

Le programme prévoit la gestion des centres d'opérations en matière de cybersécurité de la société à l'échelle mondiale, la formation, la réalisation d'exercices de simulation d'incidents liés à la cybersécurité, la mise en œuvre des politiques et des normes de la société relatives à la gestion des risques technologiques et de la cybersécurité, et l'amélioration, au besoin, des capacités de la société en matière de cybersécurité.

Recours à des conseillers externes indépendants et mobilisation du conseil

Nous maintenons et documentons également un programme de sécurité de l'information, qui prévoit l'évaluation régulière des risques par la société et des spécialistes tiers afin de cerner les menaces d'atteinte à la sécurité susceptibles de nuire à l'organisation, la détection des vulnérabilités potentielles et l'atténuation des risques de sécurité identifiés. Le programme, qui s'inspire des cadres et ensembles de normes du secteur, est conçu pour protéger la confidentialité, l'intégrité et l'accessibilité des actifs informationnels et des systèmes servant à stocker, traiter ou transmettre des informations.

Harmonisation avec un cadre ou une norme externe

Chaque année, des évaluations des risques et des audits de conformité sont réalisés, tant en interne que par des tiers indépendants, sur la base de normes pertinentes, comme le cadre de sécurité du National Institute of Standards and Technology (NIST) et les normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS), et le degré de maturité du programme est régulièrement comparé à celui des programmes mis en place par des chefs de file du secteur.

Validation

Sensibilisation et formation en matière de sécurité. Des événements et des activités de sensibilisation, comme le mois de la sensibilisation à la cybersécurité, des expositions, des vidéos, des programmes de formation et de fréquentes simulations d'hameçonnage, sont organisés tout au long de l'année. [La société] déploie continuellement des formations pour sensibiliser les membres de son personnel à l'importance de préserver la confidentialité et l'intégrité des données des clients. Toutes les nouvelles recrues doivent, dans le cadre de notre processus d'orientation, suivre une formation obligatoire sur la protection et la confidentialité des informations, et tous les membres du personnel suivent une formation annuelle à jour sur la cybersécurité.

Vous voulez en savoir plus?

Le site Web du Center for Board Matters d'EY (ey.com/us/boardmatters) donne accès à de l'information additionnelle et à des documents de leadership éclairé.

EY | Travailler ensemble pour un monde meilleur

EY contribue à un monde meilleur en créant de la valeur pour ses clients, pour ses gens, pour la société et pour la planète, tout en renforçant la confiance à l'égard des marchés financiers.

Grâce aux données, à l'intelligence artificielle et aux technologies de pointe, les équipes d'EY aident les clients à façonner l'avenir en toute confiance et proposent des solutions aux enjeux les plus pressants d'aujourd'hui et de demain.

Les équipes d'EY fournissent une gamme complète de services en certification, en consultation et en fiscalité ainsi qu'en stratégie et transactions. S'appuyant sur des connaissances sectorielles, un réseau mondial multidisciplinaire et des partenaires diversifiés de l'écosystème, les équipes d'EY sont en mesure de fournir des services dans plus de 150 pays et territoires.

EY est *All in* pour façonner l'avenir en toute confiance.

4760895

www.ey.com/fr_ca/board-matters