GUIDE ICC DE LA CYBERSÉCURITÉ À L'INTENTION DES ENTREPRISES

CHAMBRE
DE COMMERCE
INTERNATIONALE
L'organisation mondiale des entreprises

GUIDE ICC DE LA CYBERSÉCURITÉ À L'INTENTION DES ENTREPRISES

Remerciements

Le *Guide ICC de la cybersécurité à l'intention des entreprises* s'inspire du *Guide belge de la cybersécurité*, une initiative d'ICC Belgium et de la VBO-FEB ainsi que d'EY Belgique et de Microsoft Belgique, avec le concours du B-CCENTRE et d'ISACA Belgium. Bien accueilli en Belgique, ce guide a été proposé comme modèle à la Commission de l'économie numérique d'ICC afin d'être adapté à un cadre mondial, avec l'autorisation des entreprises et des organisations concernées.

ICC remercie chaleureusement les personnes ayant participé à la préparation et à la publication du guide belge ainsi que les membres du groupe de travail d'ICC sur la cybersécurité qui ont rédigé le présent guide mondial.

Copyright

© 2015, Chambre de commerce internationale (ICC)

ICC détient tous les droits d'auteur et autres droits de propriété intellectuelle du présent ouvrage collectif et encourage sa reproduction et sa diffusion, sous réserve des conditions suivantes :

- ICC doit être citée en tant que source et détenteur des droits d'auteur et le titre de l'ouvrage, « © Chambre de commerce internationale (ICC) » et, le cas échéant, l'année de publication doivent être mentionnés.
- Une autorisation écrite expresse doit être obtenue pour toute modification, adaptation ou traduction, pour tout usage commercial et pour tout usage impliquant qu'une autre personne physique ou morale est la source de l'ouvrage, ou y est associée.
- L'ouvrage ne doit pas être reproduit ou rendu accessible sur des sites web, sauf par un lien renvoyant à la page web ICC correspondante (et non au document lui-même).

Une demande d'autorisation peut être effectuée auprès d'ICC à l'adresse: ipmanagement@iccwbo.org

ICC Publication No. 450/1081-5
ISBN: 978-92-842-0387-1

TABLE DES MATIÈRES

AVANT-PROPOS

John Danilovich, secrétaire général d'ICC

Depuis près d'un siècle, la Chambre de commerce internationale (ICC) est fière de proposer aux entreprises des outils et des principes d'autodiscipline encourageant de bonnes pratiques commerciales.
En tant qu'organisation mondiale des entreprises, ICC fédère des adhérents de tous secteurs et de toutes régions. À ce titre, elle est particulièrement heureuse de publier aujourd'hui ce guide rédigé en termes simples et clairs, destiné à aider les organisations de toutes tailles à assumer leur part de responsabilité face au problème de plus en plus sérieux de la cybersécurité.

ICC a pour mission de faciliter le commerce et l'investissement, et notamment de renforcer la confiance dans l'économie numérique afin d'élargir les horizons qu'elle ouvre aux entreprises, aux consommateurs, aux pouvoirs publics et à la société en général. L'interconnectivité a non seulement transformé le marché, mais aussi le tissu social. Les bénéfices engendrés par un meilleur accès à la connaissance, à l'information, aux biens et aux services ont été rendus possibles par un internet mondial ouvert. Ce dernier doit être fiable et sûr. Toute stratégie en matière de cybersécurité doit donc être adaptée, justifiée et proportionnée, afin de préserver ces bénéfices.

La sécurité étant – à l'instar de la perfection – un objectif difficile à atteindre, fruit de multiples compromis, s'y attaquer peut aussi paraître difficile. La crainte d'une méconnaissance du sujet peut empêcher les entreprises d'évaluer les risques et de prendre les mesures nécessaires. Ce guide a pour but de vaincre l'obstacle de l'appréhension par une approche simple, expliquée étape par étape. ICC a rédigé ce *Guide de la cybersécurité à l'intention des entreprises* dans l'espoir de toucher un vaste public, avec à l'esprit ses plus de six millions d'adhérents. Loin d'être destiné aux seules équipes informatiques, il se veut accessible aux dirigeants, aux cadres et aux membres du personnel des entreprises, et devrait être communiqué aux partenaires commerciaux des chaînes d'approvisionnement de biens et de services ainsi qu'au secteur public, afin de renforcer à tous les niveaux la résilience aux cyberincidents.

Ce guide doit être diffusé dans les plus de 130 pays que couvre le réseau mondial d'ICC par ses comités nationaux et ses adhérents – entreprises, associations économiques et membres de la Fédération mondiale des chambres de commerce. ICC est convaincue que l'action collective mondiale de son réseau et de ses partenaires peut apporter une contribution essentielle à la réduction des cyberrisques encourus par les entreprises et par l'ensemble de la société.

LA CYBERSÉCURITÉ PASSE D'ABORD PAR VOUS

Les technologies de l'information et de la communication permettent aujourd'hui aux entreprises de toutes tailles d'innover, d'accéder à de nouveaux marchés et de réaliser des gains d'efficacité bénéficiant à leurs clients et à la société. Leurs pratiques et leurs politiques sont pourtant de plus en plus bousculées par le besoin de s'adapter aux effets directs et indirects de l'omniprésence des environnements de communication et des flux d'information en réseau nécessaires à la fourniture de biens et de services. De nombreuses entreprises adoptent les récentes technologies de l'information et de la communication sans pleinement comprendre que cela implique aussi de gérer de nouveaux types de risques. Le présent guide a pour objet de combler cette lacune en expliquant comment les entreprises de toutes tailles peuvent identifier et gérer les cyberrisques.

Les failles de cybersécurité font souvent l'actualité de la presse, qui relate les intrusions dans les systèmes de grandes ou petites entreprises d'acteurs malveillants agissant apparemment à leur guise et sans obstacle. Les entreprises sont aujourd'hui exposées à des sources de risques toujours plus nombreuses[1] car criminels, pirates informatiques, acteurs étatiques et concurrents emploient des moyens de plus en plus sophistiqués pour exploiter les faiblesses des technologies modernes de l'information et de la communication. La combinaison des systèmes informatiques et de divers équipements externes[2] accroît le niveau de complexité et les menaces qui pèsent sur ces systèmes. En plus des menaces extérieures, les entreprises doivent gérer les risques d'attaques internes de leurs systèmes d'information par des acteurs capables de corrompre leurs données ou de tirer profit de leurs ressources, confortablement installés chez eux ou au café du coin. Il est donc essentiel pour elles – et ce quelle que soit leur taille – d'être en mesure d'identifier les cyberrisques qu'elles courent et de gérer efficacement les menaces à l'encontre de leurs systèmes d'information. Tous les membres de l'équipe dirigeante, ainsi que les cadres de tous niveaux, doivent cependant être conscients que la gestion du cyberrisque est un processus permanent au sein duquel il n'existe ni n'existera jamais de sécurité absolue.

Contrairement à de nombreux autres problèmes auxquels les entreprises sont confrontées, la gestion du cyberrisque n'a pas de solution simple. Elle exige de la part de l'équipe dirigeante une attention constante, une bonne tolérance aux mauvaises nouvelles et une discipline de communication claire. Bon nombre d'excellentes ressources fournissant des explications détaillées sur les principales cybermenaces sont disponibles, mais les documents pouvant aider les dirigeants d'entreprise dans leur approche de la

1 Parmi les menaces croissantes à l'encontre de la cybersécurité figurent par exemple les maliciels (tels que logiciels d'intrusion, injection de code, kits d'exploitation, vers, chevaux de Troie, etc.), les dénis de services, les violations de données et autres. Pour un point sur la situation, voir par ex. *ENISA Threat Landscape 2014*, EL 2014, sur https://www.enisa.europa.eu

2 Tels que téléphones portables, modems, terminaux de paiement, mises à jour automatiques de logiciels, systèmes industriels de contrôle, interaction fournisseur/client, internet des objets.

cybersécurité demeurent rares. **Ce guide a pour objet d'aider les dirigeants, que leur organisation soit grande ou petite, à interagir avec leurs responsables des technologies de l'information et à élaborer des pratiques de gestion du cyberrisque**.

Il est possible d'améliorer la cybersécurité d'une organisation par un processus de gestion du risque – la clé étant la gestion. Du fait de l'évolution constante des technologies et des vecteurs de menace, les systèmes d'information de l'entreprise ne seront jamais finis, et ne pourront jamais non plus être totalement sécurisés. Travailler efficacement dans un tel environnement exige une approche à long terme de la gestion du risque – sans résultat définitif. Les initiatives en matière de cybersécurité laisseront les dirigeants d'entreprise frustrés s'ils n'adaptent pas leurs attentes à la nature de la tâche à accomplir. Et si des limites adéquates ne sont pas posées, la quête d'une réduction des cyber-risques peut vite consommer toutes les ressources disponibles de l'entreprise. Il est donc primordial d'aborder la gestion du cyberrisque comme un processus permettant à l'entreprise de comprendre et de hiérarchiser ce qui compte le plus pour elle (biens corporels et actifs informationnels).

Il est essentiel d'avoir conscience que **sans précautions adéquates, l'internet, les réseaux d'information et les équipements de l'entreprise ne sont pas en sécurité**. Les systèmes d'information actuels des entreprises constituent des cibles pour divers acteurs malveillants. L'on peut se référer pour fixer les attentes des responsables de la gestion du cyberrisque à un refrain simple : « Si un élément ayant de la valeur est en ligne, il est en danger et sera vraisemblablement compromis. » Heureusement, les éléments qui ont de la valeur aux yeux d'acteurs malveillants ne sont pas toujours ceux jugés les plus précieux par l'entreprise elle-même (tels qu'actifs financiers, secrets commerciaux et informations relatives aux clients). Il existe des techniques et des processus susceptibles de contribuer à réduire les risques, mais un acteur malveillant déterminé profitera toujours du maillon le plus faible des systèmes interconnectés. Toute entreprise présente de nombreuses vulnérabilités potentielles (organisationnelles, humaines et techniques). Malgré tous les efforts des fournisseurs de technologies et de services et des employés de votre organisation, aucune sécurité absolue ne peut être assurée. Le processus de gestion du cyberrisque doit donc se fonder sur une évaluation, par rapport à ses actifs prioritaires, des faiblesses de l'entreprise et des menaces particulières auxquelles elle est exposée.

Malgré le triste tableau que nous venons de brosser, les entreprises de toutes tailles peuvent développer et maintenir des capacités organisationnelles clés pour une bonne gestion du cyberrisque.

- Premièrement, l'équipe dirigeante doit lancer une analyse du risque et hiérarchiser les actifs ayant le plus besoin d'être protégés.
- Deuxièmement, un process de décision et de responsabilité doit être mis en place afin de prendre les mesures nécessaires et de veiller à ce que l'entreprise applique les meilleures pratiques en matière de sécurité de l'information.
- Troisièmement, l'entreprise doit être préparée à détecter les cyberévénements et à y réagir – en interne et en externe – par des processus organisationnels institutionnalisés.

La réaction aux incidents exige une communication renforcée entre pairs ainsi qu'avec les acteurs étatiques compétents, les clients et même les concurrents. Se préparer à l'avance à tout cyberévénement permet de s'assurer que le problème initial ne sera pas aggravé lors de la réaction de l'entreprise par des erreurs qui auraient pu être évitées. Enfin, des mécanismes permettant de tirer la leçon des cyberincidents et de modifier les pratiques en cause sont essentiels pour inspirer les changements institutionnels nécessaires à l'adoption par l'entreprise entière d'une saine gestion du cyberrisque.

COMMENT UTILISER CE GUIDE

Au cours des dix dernières années, pouvoirs publics, organisations et personnes privées ont rédigé d'innombrables textes sur les réponses à apporter au problème de la sécurité de l'information dans le cyberespace. Il existe tant de documents et de directives qu'il peut être difficile de savoir par où commencer et d'identifier les lectures les plus utiles dans le cas précis de votre entreprise. L'on trouvera notamment dans cette documentation foisonnante (par ordre de spécificité croissante) :

- **des lignes directrices** – visions de haut niveau traitant de préoccupations en matière de cybersécurité et énonçant des principes à l'intention de personnes morales ou physiques. Exemples : Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information, etc.
- **des stratégies nationales** – documents se fondant souvent sur des lignes directrices et définissant une approche de la cybersécurité adaptée à un contexte national ou juridique particulier. Exemples : International Strategy to Secure Cyberspace[3], National strategies from Europe and other states[4], etc.
- **des cadres** – étape suivante des stratégies nationales, cataloguant des ressources hiérarchisées ou évaluées afin d'aider les organisations à évaluer leur maturité et leur progrès en matière de gestion du cyberrisque. Exemples : National Institute of Standards and Technology (NIST) Cybersecurity Framework[5], etc.
- **des normes de conduite** – documents orientant ou régissant les processus organisationnels afin d'assurer la mise en œuvre efficace et cohérente de pratiques d'excellence en matière de cybersécurité. Exemples : normes de procédure ISO 27001, 27002, 27032, normes de sécurité PCI, etc.
- **des standards techniques** – spécifications détaillées pour la mise en œuvre d'interfaces répondant à des exigences d'interopérabilité particulières. Exemples : HTTPS, AES, EMV, normes de paiement PCI, etc.

Le présent guide, qui s'inspire des lignes directrices mondiales et des stratégies nationales en matière de cybersécurité, propose aux entreprises, sous une forme simple et claire, un cadre de réflexion sur la question de la sécurité en ligne – avec, premièrement, une série de **cinq principes** applicables par les organisations de toutes tailles à leur approche du cyberrisque. Il identifie, en deuxième lieu, **six actions clés** que les entreprises devraient mener en priorité, en se fondant sur des pratiques d'excellence et des documents de diverses sources. Le guide explique ensuite **comment traduire les cinq principes initiaux en une politique**, afin d'orienter au sein de l'entreprise le développement des activités de gestion du cyberrisque. Ces conseils sont complétés par une annexe numérique évolutive recensant des ressources plus spécifiques qui s'enrichira à mesure que paraîtront de nouveaux textes – normes de conduite, standards techniques et autres. Bien qu'il n'existe pas de sécurité absolue, les principes de gestion du cyberrisque exposés ici aideront les entreprises à relever le défi de la sécurité de l'information dans un environnement en perpétuelle mutation. Ce guide leur sera utile à titre individuel, mais, au-delà de cet intérêt immédiat, elles doivent aussi le partager avec tous les acteurs de leur chaîne de relations afin de mieux sécuriser tous les points d'entrée et d'échange de leurs systèmes et activités.

3 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

4 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

5 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

COMMENT UTILISER CE GUIDE

PRINCIPES CLÉS DE SÉCURITÉ

L'approche de la sécurité de l'information peut varier d'une entreprise à l'autre selon divers facteurs[6], mais il existe un certain nombre de principes généraux sur lesquels doivent reposer les pratiques de gestion de la sécurité de l'information de toutes les entreprises, indépendamment de leur taille et de leur secteur. Ce guide présente **cinq principes clés**, classés en deux catégories :

A. Vision et attitude

B. Organisation et processus

Ces principes sont complétés par une série de **six actions de sécurité** essentielles, puis par **cinq éléments de base pour mettre en œuvre les principes** exposés et étayer la politique de sécurité de l'information de l'entreprise.

Collectivement, les principes et les actions proposés dans ce guide amélioreront la résilience de l'entreprise face aux cybermenaces et limiteront les perturbations en cas d'incident de sécurité.

A. VISION ET ATTITUDE

Principe 1: Concentrez-vous sur l'information, pas sur la technologie

Vous êtes la première ligne de défense de votre entreprise contre les cybermenaces et vous contribuez à donner le ton pour son approche de la sécurité de l'information. À ce titre, vous devez envisager celle-ci dans son sens le plus large, et non pas seulement en termes de technologies de l'information.

La sécurité de l'information englobe une combinaison de personnes, de processus et de technologies et ne concerne donc pas uniquement les technologies de l'information, mais l'ensemble de l'entreprise. La mise en œuvre de mesures de sécurité ne doit pas être le fait des seuls services informatiques, mais toucher à toutes les activités de l'organisation.

Le périmètre de la sécurité de l'information s'étend par conséquent aux ressources humaines, aux produits, aux installations, aux processus, aux politiques, aux procédures, aux systèmes, aux technologies, aux équipements, aux réseaux et aux données.

L'humain est la clé. Identifier et gérer les vulnérabilités des actifs informationnels et les menaces qui pèsent sur eux peut être une énorme tâche. L'expérience[7] montre néanmoins que 35 % des incidents de sécurité résultent d'une erreur humaine plutôt que d'une attaque délibérée. Et plus de la moitié des incidents restants sont dus à des attaques **qui auraient pu être évitées** si l'information avait été traitée de manière plus sécurisée.

6 Y compris, entre autres, la nature de l'activité, le niveau de risque, les facteurs environnementaux, le niveau d'interconnexion, les exigences réglementaires et la taille de l'entreprise.

7 *EY 2012 Global Information Security Survey – Fighting to close the gap*

Vous devez donc concentrer vos efforts sur la protection de vos informations et de vos systèmes les plus précieux, dans le cas desquels une atteinte à la confidentialité, à l'intégrité ou à la disponibilité porterait gravement préjudice à votre entreprise. Cela ne signifie pas que la sécurité de vos autres actifs informationnels puisse être ignorée, mais qu'une approche de la sécurité de l'information essentiellement fondée sur l'analyse du risque encouru par les « joyaux de la couronne » est en pratique efficace. Cette approche intègre également le fait qu'une élimination du risque à 100 % n'est ni possible, ni nécessaire, compte tenu de son coût.

Principe 2: Instaurez une attitude de résilience

L'objectif doit être de rendre l'entreprise résiliente face aux risques de perte ou de compromission de l'information. Les entreprises sont soumises à de nombreuses lois et réglementations dont beaucoup exigent la mise en œuvre de contrôles de sécurité appropriés. Se conformer aux lois, réglementations et normes peut engendrer une amélioration de la sécurité de l'information, mais peut aussi conduire à s'estimer satisfait une fois cet objectif atteint. Les menaces à l'encontre de la sécurité évoluent cependant bien plus vite que les lois et réglementations, ce qui rend mouvante la cible des activités de gestion du risque. Les politiques et les procédures de l'entreprise peuvent donc vite devenir obsolètes ou tout simplement inefficaces en pratique.

Une évaluation périodique de la résilience de l'entreprise face aux cybermenaces et vulnérabilités est indispensable pour mesurer les progrès de la réalisation de ses objectifs de gestion du risque et la pertinence de ses mesures de cybersécurité. Cette évaluation peut se faire au moyen d'analyses et d'audits internes et / ou externes comprenant notamment des tests d'intrusion et des dispositifs de détection des incidents. Les équipes informatiques ne doivent pas être les uniques responsables de la cybersécurité et les acteurs décisionnaires doivent s'impliquer non seulement dans l'identification des problèmes, mais aussi à long terme dans la mise en place d'un écosystème sain. Les évaluations périodiques ne prennent cependant tout leur sens que lorsqu'elles sont utilisées pour améliorer la culture de l'entreprise et l'attitude des employés vis-à-vis des pratiques de gestion du cyberrisque.

Un état d'esprit favorisant la résilience des systèmes d'information est surtout essentiel lorsque de nouveaux équipements ou solutions sont adoptés par l'entreprise. Dans ce cas, des mesures de sécurité appropriées doivent être envisagées aussi tôt que possible au cours du processus, dans l'idéal dès la phase d'identification des besoins de l'entreprise. Une telle intégration de la sécurité dans la conception des projets permet de donner aux employés à l'origine de la mise en œuvre des innovations les moyens de se focaliser sur la gestion du cyberrisque.

B. ORGANISATION ET PROCESSUS

Principe 3: Préparez-vous à réagir

Même les entreprises les mieux protégées connaîtront à un moment ou à un autre une atteinte à la sécurité de l'information. Nous vivons dans un environnement où la question n'est de savoir **si**, mais **quand** un incident se produira. Par conséquent, la manière dont l'entreprise **réagira** est le critère selon lequel **vous** serez jugé.

Afin de réduire l'impact des cyberincidents sur leurs activités, les entreprises doivent élaborer, en plus de mesures de réaction technique, des plans de réaction organisationnelle. Ces derniers doivent poser des jalons afin d'aider l'équipe dirigeante à savoir quand se tourner vers des spécialistes extérieurs pour contenir un incident de sécurité et y remédier, et quand contacter d'autres tiers (y compris les autorités policières et judiciaires ou les organismes publics de surveillance). N'oubliez pas qu'avertir les autorités compétentes est un moyen d'améliorer le paysage sécuritaire global et peut aussi être obligatoire, dans certains cas, sous peine de contrevenir à la réglementation et de s'exposer à des amendes. Une bonne gestion de la réaction à un incident doit également inclure une stratégie de communication (interne et externe), élément qui peut vous valoir d'être cité en exemple de réussite dans le cadre de programmes universitaires plutôt que de manière embarrassante à la une de la presse.

Bien que les activités internes de gestion du risque soient essentielles, vous devez aussi prendre le temps de maintenir des contacts avec vos pairs et vos partenaires, dans le secteur d'activité de votre entreprise, ainsi qu'avec le reste de la communauté économique et avec les autorités policières et judiciaires, afin de contribuer à la compréhension des menaces existantes et émergentes et de bâtir des relations qui vous seront précieuses en cas d'incident.

Principe 4: Montrez que vous prenez vos responsabilités

Afin d'assurer une gestion efficace de la sécurité de l'information, les dirigeants doivent comprendre que cette gestion constitue un élément essentiel du succès de l'entreprise et lui apporter tout leur soutien. **Vous** et votre équipe dirigeante devez vous engager de manière visible dans le pilotage et la supervision de la politique de gestion du cyberrisque de votre

organisation. Il est de votre devoir de veiller à ce que des ressources adéquates – tant humaines que financières – soient allouées à la protection de ses actifs. Mais les ressources ne sont pas tout : les entreprises, petites ou grandes, doivent créer une fonction de responsable de la sécurité de l'information afin de permettre une réaction aux cybermenaces et vulnérabilités à l'échelle de l'ensemble de l'organisation.

Des rapports sur l'efficacité et la pertinence des mesures de sécurité devraient être formellement adressés à la personne la plus haut placée de votre entreprise et, au moins une fois par an, à l'équipe dirigeante, aux auditeurs et au conseil d'administration. Ces rapports réguliers – fondés sur divers indicateurs et résultats chiffrés – devraient alimenter le processus de prise de décision en matière de politique et d'investissement dans la sécurité de l'information, et fournir des indications sur le degré de protection des actifs de l'entreprise.

Bien que le personnel soit souvent désigné comme le *maillon faible* de la sécurité de l'information, vous pouvez en faire votre *meilleur atout sécuritaire* en le sensibilisant au problème et en lui faisant acquérir de réelles compétences en la matière.

Principe 5: Mettez votre vision en œuvre

Lire ce guide ne suffit pas – vous devez mettre en pratique la vision de la gestion du cyberrisque de votre entreprise en élaborant (ou en révisant) différentes politiques de sécurité de l'information. Celles-ci doivent établir un cadre de référence normalisé destiné à orienter les activités de sécurité de tous les services et de tout le personnel de l'entreprise, tout en renforçant sa sensibilisation au sujet.

En général, le document exposant la politique de sécurité et les directives et normes qui l'accompagnent sont rassemblés en un cadre stratégique, ensuite traduit en procédures opérationnelles normales. Avec l'intégration de plus en plus fréquente de prestataires de services extérieurs dans les chaînes de valeur de l'entreprise, cette dernière doit toutefois prendre conscience de la manière dont ses actifs informationnels circulent parmi différents tiers et en sont dépendants. Si ces tiers ne protègent pas correctement vos informations (ou les systèmes d'information sur lesquels vous vous reposez), **leur** incident de sécurité peut présenter un risque sérieux pour **vos** opérations commerciales, votre réputation et votre valeur de marque. Vous devez encourager vos fournisseurs à adopter au minimum les principes relatifs à l'information et à sa sécurité en vigueur dans votre entreprise, mener le cas échéant des audits ou demander aux prestataires de services de détailler leurs pratiques en matière de sécurité de l'information afin d'obtenir des assurances solides sur leur qualité.

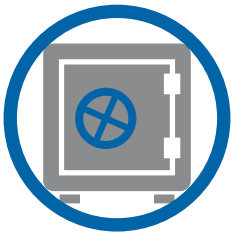
Les tiers ne sont toutefois pas qu'une source de risque – certains peuvent vous aider à le réduire et à atteindre des objectifs vitaux en matière de gestion du cyberrisque. Les fournisseurs de services de technologies de l'information peuvent contribuer à l'amélioration de votre infrastructure de gestion du cyberrisque, notamment grâce à des audits et à des évaluations de la sécurité et à l'utilisation

d'équipements et de solutions de sécurité de l'information ou à des services, que ce soit sur site, en externe ou en faisant appel au cloud computing[8].

La liste d'actions qui suit contient une série de mesures pratiques que les entreprises de toutes tailles peuvent prendre pour réduire le risque lié aux incidents de cybersécurité. Bien qu'elle ne soit ni complète ni exhaustive, veiller à ce que votre entreprise suive les étapes qui y figurent l'engagera dans la voie de l'excellence en matière de sécurité de l'information.

Vous devez avoir à l'esprit que la gestion du cyberrisque est un processus au long cours. Une fois ces premières actions lancées, consultez le portail web associé au présent guide afin de trouver les normes et les ressources qui vous aideront à prendre encore d'autres mesures afin de renforcer la résilience de votre programme de sécurité de l'information.

8 Les services faisant appel au cloud computing, ou « services cloud », sont des solutions dans le cadre desquelles l'entreprise a recours à un fournisseur de services externe pour stocker, traiter ou gérer des données via un réseau tels que l'internet, avec un haut niveau de flexibilité et de suivi en temps réel.



Action 1: Sauvegardez vos informations et validez le processus de récupération

Veillez à ce que vos informations soient protégées par une procédure de sauvegarde – avant que votre entreprise ne soit victime d'une atteinte à la sécurité de l'information et que des données soient volées, altérées, effacées ou perdues. Une simple copie de sauvegarde ne suffit pas[9]. Une bonne gestion des processus de sauvegarde inclut la validation du contenu de l'information et des données des fichiers sauvegardés ainsi que des tests de récupération. Si le stockage de certaines données est confié à des tiers (services cloud, par ex.), assurez-vous qu'elles fassent également l'objet de mesures de sauvegarde.

N'oubliez pas que les supports matériels tels que CD, bandes magnétiques ou disques durs utilisés pour stocker les données sauvegardées sont aussi vulnérables aux risques. Les sauvegardes doivent bénéficier du même niveau de protection que les données sources, en particulier en ce qui concerne leur sécurité matérielle, car ces éléments sont faciles à transporter.

Action 2: Mettez à jour vos systèmes informatiques

Les systèmes et logiciels de toutes sortes, y compris les appareils et les équipements de réseau, doivent être mis à jour chaque fois que des correctifs ou des mises à niveau de micrologiciel sont disponibles. Ces mises à niveau et correctifs de sécurité remédient à des vulnérabilités des systèmes dont des attaquants peuvent profiter. Bon nombre d'entre eux parviennent à exploiter des failles de sécurité pour lesquelles des mises à jour étaientdisponibles, souvent même depuis plus d'un an.

Utilisez autant que possible des services de mise à jour automatique, en particulier pour les systèmes de sécurité tels que les programmes antimaliciels, les outils de filtrage web et les systèmes de détection d'intrusion. Les processus de mise à jour automatique peuvent contribuer à faire en sorte que les utilisateurs appliquent des mises à jour de logiciels de sécurité valides provenant directement du fournisseur d'origine.

9 Une procédure de sauvegarde est un processus technique qui doit être correctement géré. Se contenter d'utiliser simultanément plusieurs supports de stockage sur un même site, par exemple, ne constitue pas une procédure de sauvegarde suffisante. Une politique de sauvegarde efficace doit tenir compte de multiples types de risques, dont la perte de données et la perte du site d'activité, qui exigent que des copies de sauvegarde soient physiquement stockées hors site.

Action 3: Investissez dans la formation

Il est essentiel que tout le personnel de votre entreprise possède des connaissances de base sur les cybermenaces et les questions de sécurité, et que ces connaissances soient en permanence entretenues. La formation du personnel[10] garantit que tous ceux qui ont accès aux données et aux systèmes d'information soient conscients de leurs responsabilités quotidiennes dans leur traitement et dans leur protection, ainsi que dans le soutien aux activités de sécurité de l'information de l'entreprise. Sans une formation appropriée, les employés peuvent rapidement devenir une source de risques au sein de l'entreprise et être à l'origine d'incidents de sécurité ou de vulnérabilités dont des adversaires peuvent profiter pour contourner vos mesures de sécurité.

Vous **pouvez** établir dans votre entreprise une culture de gestion du cyberrisque. Investir dans la formation renforcera les messages sur la sécurité de l'information destinés au personnel et développera ses qualités et ses compétences en matière de sécurité.

Action 4: Surveillez votre environnement informatique

Les entreprises doivent déployer des systèmes et des processus destinés à les alerter en cas d'incident de sécurité. Elles en sont trop souvent ignorantes et certaines peuvent subir des violations ou des infections pendant des mois, voire des années, avant que l'intrusion soit détectée[11].

Différentes solutions technologiques existent afin de vous aider dans cette tâche, dont des systèmes de détection et de prévention des intrusions et de gestion des incidents de sécurité. Les installer n'est cependant pas suffisant. Pour en tirer pleinement parti, il est également nécessaire de surveiller et d'analyser en permanence leurs résultats.

10 Vous trouverez notamment des informations générales sur la cybersécurité et la sensibilisation des utilisateurs sur www.staysafeonline.org. http://www.enisa.europa.eu/media/multimedia/material, une initiative de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). L'utilisation de toutes ces informations, vidéos et infographies est autorisée à des fins éducatives au sein de l'entreprise.

11 http://www.verizonenterprise.com/DBIR/2013/ – *Verizon 2013 Data Breach Investigations Report*

De nombreuses entreprises peuvent ne pas disposer en interne de l'expertise ou des ressources nécessaires pour surveiller leurs systèmes et leurs processus les plus vitaux. Des services de sécurité sur site ou gérés en externe sont disponibles auprès de divers prestataires selon différents modèles économiques, dont des technologies et services faisant appel au cloud computing. Trouvez celui qui convient le mieux à votre organisation et demandez à des tiers expérimentés conseils, assistance et soutien afin d'inclure dans vos contrats des clauses appropriées.

Si votre entreprise est victime d'un cyberincident, envisagez de le signaler aux organismes publics[12] et aux associations sectorielles compétentes – communiquer avec d'autres peut vous aider à déterminer si vous êtes la cible d'un événement isolé ou d'une plus vaste série d'attaques[13]. Établir des contacts permet souvent de recueillir des informations et des conseils susceptibles d'aider l'entreprise à mettre en place des contre-mesures efficaces.

Action 5: Multipliez les lignes de défense pour réduire les risques

La sécurisation du périmètre de réseau et le contrôle d'accès traditionnel ne suffisent plus, surtout quand le système d'information est connecté à l'internet et à des prestataires de services internet, des services externes, des services cloud, des fournisseurs et des partenaires, ainsi qu'à des appareils mobiles qui se trouvent hors de portée et de contrôle de l'entreprise. Se protéger efficacement contre les virus, les maliciels, les équipements malveillants et les pirates informatiques exige plusieurs niveaux de mesures défensives afin de réduire le risque d'un incident de sécurité de l'information. Combiner de multiples techniques[14] pour contrer le cyberrisque peut significativement réduire la probabilité de voir une atteinte minime se transformer en un grave incident.

De multiples lignes de défense permettent de restreindre la liberté d'action des adversaires et améliorent les chances de détection par les systèmes de surveillance de l'entreprise.

S'assurer contre les cyberrisques peut être pour l'entreprise un moyen de limiter les conséquences financières d'un incident, mais aussi de gérer proactivement les menaces et de renforcer sa gestion interne du risque.

12 Les victimes de (cyber) délits devraient aussi porter plainte auprès des autorités policières et judiciaires compétentes. La police locale est en général le meilleur interlocuteur en ce qui concerne la criminalité traditionnelle, mais d'autres services peuvent être spécialisés dans la cybercriminalité (piratage, sabotage, espionnage).

13 Les attaques peuvent être horizontales (des entreprises d'un même secteur sont visées) ou verticales (des sous-traitants sont visés), ou résulter d'une menace touchant spécifiquement un élément particulier d'un logiciel ou d'un matériel.

14 Y compris, pour n'en citer que quelques-unes, le filtrage web, les antivirus, la protection proactive contre les maliciels, les pare-feux, de solides politiques de sécurité et une formation des utilisateurs.

Action 6: Préparez-vous à faire face aux incidents

La gestion du risque ne consiste pas seulement à réduire la probabilité d'un incident, mais aussi à limiter les dégâts lorsqu'il survient. Cela implique d'être prêt à enquêter rapidement sur l'incident – en veillant à ce que les ressources nécessaires soient disponibles et à ce que les systèmes et les processus soient programmés pour capter les informations critiques. Si l'incident est dû à l'intrusion d'un maliciel, celui-ci doit être éliminé. Il convient aussi de disposer d'un plan organisationnel pour prendre rapidement les bonnes décisions et coordonner les actions nécessaires pour reprendre le contrôle de la situation. Qui doit réagir et comment ? Votre équipe peut influer sur le résultat par des actions bien conçues et une communication efficace.

Et enfin, se préparer à l'avance peut circonscrire certaines des conséquences les plus dommageables d'un incident – perte d'opérabilité, inaccessibilité des données, impossibilité de reprendre l'exploitation sans délai. Planifier la continuité d'activité et la récupération réduit les pertes en concentrant les efforts sur les priorités de l'entreprise et en maintenant un bon état de préparation.

MISE EN ŒUVRE DES PRINCIPES DANS LE CADRE D'UNE POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Les dirigeants d'entreprise ont fréquemment pour tâche de traduire les principes proposés dans des documents comme celui-ci en politiques et en pratiques faisant sens pour leur organisation. L'objectif de ce chapitre est de leur faciliter le travail. Reprenant les cinq principes clés de sécurité précédemment exposés, les éléments ci-dessous posent les bases de l'élaboration de bonnes politiques et pratiques de gestion du cyberrisque.

Concentrez-vous sur l'information, pas sur la technologie

- Créez une fonction et nommez-y une personne chargée de diriger et de faciliter les initiatives touchant à la sécurité de l'information, tout en faisant en sorte que la responsabilité en matière de sécurité demeure partagée par l'ensemble de l'entreprise.
- Lorsqu'elle planifie la manière d'atteindre ses objectifs de sécurité de l'information, l'entreprise doit déterminer :
  - ce qui sera fait
  - quelles seront les ressources nécessaires
  - qui sera responsable
  - quand cela sera fait
  - comment les résultats seront évalués[15].
- Au cas où votre entreprise ne disposerait pas en interne d'une expérience suffisante de la sécurité, faites appel à des informations complémentaires et à des experts en cybersécurité afin de vous aider à intégrer la sécurité de l'information dans la conception de vos processus internes et de vos systèmes d'information.

Instaurez une attitude de résilience

- Les activités touchant à la sécurité de l'information devraient être cohérentes avec les actions de mise en conformité et les autres efforts de réduction des risques – et si possible y être intégrées – afin d'éviter que les initiatives et les responsabilités fassent double emploi.
- L'aversion pour le risque ne devrait pas bloquer l'adoption de nouvelles technologies. Une bonne approche de la sécurité de l'information peut non seulement aider l'entreprise à atteindre ses objectifs de gestion du cyberrisque, mais aussi la préparer à l'introduction de technologies innovantes.

15 ISO/IEC 27001:2013

- Veillez à ce que la sécurité soit prise en compte dans tous les projets menés par votre entreprise, et en particulier les nouveaux. Lorsqu'elle est intégrée dès le départ, avec l'implication active de l'entreprise, la sécurité n'augmente pas significativement le coût et la durée de mise en œuvre des projets. Quand elle est ajoutée après coup, ou – dans le pire des cas – à la suite d'un incident, les dépassements de coûts, délais et autres conséquences augmentent de plusieurs ordres de grandeur.
- Déterminez quels équipements – et surtout quels appareils mobiles de votre personnel ou de vos partenaires commerciaux – peuvent être autorisés à accéder au réseau et / ou aux informations de votre entreprise[16], et étudiez la manière de gérer les logiciels et les options de sécurité des équipements appartenant à l'entreprise.
- Évaluez l'accès aux données afin de vérifier que des contrôles soient en place pour préserver leur confidentialité, leur intégrité et leur disponibilité.
- Les manageurs devraient recevoir, vérifier et valider les utilisateurs (internes et externes) qui ont accès aux applications et aux informations de leurs services respectifs – l'accès aux données et aux systèmes d'information est une responsabilité et un risque et il est donc recommandé de le contrôler.
- Élaborez des procédures de signalement des pertes ou vols d'équipement et, si possible, des fonctions de suppression à distance des données pour effacer toutes les informations de l'entreprise contenues dans les équipements perdus ou volés.

Préparez-vous à réagir

- Tout le monde commet des erreurs et les entreprises qui savent faire de chaque incident une occasion de réévaluer ouvertement leur sécurité de l'information peuvent créer une culture dans laquelle les employés n'ont pas peur de signaler les incidents quand il en survient.
- Autoriser certains employés à partager des informations appropriées avec des pairs et avec d'autres acteurs de votre secteur d'activité aide à élaborer des pratiques exemplaires et à donner l'alerte en cas d'attaque potentielle.
- Désignez un responsable afin d'assurer dès le départ une sauvegarde adéquate des éléments de preuve lors d'incidents de sécurité et surtout en cas d'actes de cybercriminalité[17].
- Déterminez quand et comment signaler les incidents de sécurité aux centre d'alerte et de réaction aux attaques informatiques (CERT – Cyber Emergency Response Team), aux organismes publics ou aux autorités policières et judiciaires.

16 Exigez des utilisateurs qu'ils configurent les options de sécurité de leurs appareils mobiles de manière à empêcher que des criminels les utilisent pour voler des informations.

17 Des lignes directrices sur l'acquisition de données à des fins d'enquête par les équipes informatiques lors d'incidents de sécurité ou d'infections par des maliciels sont disponibles en ligne sur : http://cert.europa.eu/cert/plainedition/en/cert_about.html

Le leadership compte

- Les employés doivent être considérés comme responsables de l'information et de sa protection et devaient avoir le niveau d'autorité, la possibilité d'avoir accès à la direction générale, les outils et la formation nécessaires pour assumer leurs responsabilités et affronter les menaces qu'ils peuvent rencontrer[18].
- Les petites entreprises doivent disposer d'une personne, en interne ou en externe, qui contrôle régulièrement la pertinence des mesures de gestion du cyberrisque et endosse formellement la responsabilité de la sécurité de l'information. Ce rôle n'a pas besoin d'être exercé à plein temps, mais il est important et peut s'avérer crucial pour la survie de l'entreprise.
- Dans les grandes entreprises, la répartition des fonctions, des rôles et des responsabilités doit délibérément viser à combiner un certain nombre de personnes et de groupes de travail et comités (virtuels). Chaque membre de l'équipe doit connaître avec précision ses responsabilités. Il est donc essentiel que la documentation et la communication soient à la hauteur.

Mettez votre vision en œuvre

- Contrôlez l'accès à votre réseau interne (et depuis ce réseau), en hiérarchisant l'accès aux services et aux ressources essentiels pour les besoins de l'entreprise et des employés[19].
- Instaurez l'utilisation de mots de passe forts et envisagez la mise en place de méthodes d'authentification forte[20] exigeant plus d'informations qu'un simple mot de passe.
- Utilisez le chiffrement, au besoin, pour sécuriser les données stockées et en transit[21], surtout en ce qui concerne les connexions au réseau public et les appareils mobiles tels qu'ordinateurs portables, clés USB et smartphones, que l'on peut facilement perdre ou se faire voler.

18 Une importante menace à laquelle les employés doivent être formés est l'ingénierie sociale. Cette technique consiste à manipuler les personnes afin d'obtenir d'elles qu'elles exécutent des actions entraînant la divulgation d'informations sensibles ou confidentielles.

19 Envisagez de filtrer les services et les sites web qui augmentent les risques encourus par les ressources de l'entreprise, tels que le partage de fichiers entre pairs et les sites pornographiques, par exemple. Les règles de filtrage devraient être transparentes pour tous les utilisateurs au sein de l'entreprise et comprendre un processus de déblocage des sites légitimes dont l'accès pourrait avoir été refusé par inadvertance.

20 L'authentification multifactorielle utilise une combinaison d'éléments, par exemple quelque chose que je connais (par ex. mot de passe ou code PIN), quelque chose que j'ai (par ex. carte à puce ou SMS) et quelque chose que je suis (par ex. empreinte digitale ou scanner de l'iris).

21 Les courriels envoyés par internet, par exemple, étant souvent en clair, les entreprises devraient envisager des méthodes de chiffrement quand des informations sensibles sont transmises.

MISE EN ŒUVRE DES PRINCIPES DANS LE CADRE D'UNE POLITIQUE DE SÉCURITÉ DE L'INFORMATION

- Établissez une politique détaillée de sauvegarde et d'archivage conforme aux exigences légales et réglementaires sur la conservation d'informations, précisant :
  - quelles données doivent être sauvegardées, et comment
  - à quelle fréquence les sauvegardes doivent être faites
  - qui est responsable de leur création et de la validation de leur contenu
  - où et comment elles doivent être stockées
  - qui y aura accès
  - comment fonctionnent (et sont testées) les procédures de récupération.
- Élaborez des programmes de formation et de sensibilisation à la sécurité de l'information, y compris sur des sujets tels que :
  - communiquer de manière sûre et responsable
  - utiliser à bon escient les médias sociaux
  - transférer les fichiers numériques en toute sécurité
  - bien utiliser les mots de passe
  - éviter de perdre des informations importantes
  - veiller à ce que seules les personnes autorisées aient accès à vos données
  - se protéger des virus et autres maliciels
  - qui alerter lorsque l'on constate un incident de sécurité potentiel
  - comment ne pas se faire piéger et divulguer des informations.

QUESTIONNAIRE D'AUTOÉVALUATION EN MATIÈRE DE SÉCURITÉ

Les équipes dirigeantes trouveront ci-dessous une liste de contrôle, simple et claire, destinée à les orienter dans l'évaluation des capacités de cyberrésilience de leur entreprise et à leur permettre de poser les bonnes questions aux différents participants aux initiatives en la matière. Cet outil a été conçu pour les aider à identifier les forces et les faiblesses de leur organisation – ainsi qu'à trouver des pistes d'amélioration.

Ce questionnaire d'autoévaluation peut également être utilisé comme liste de contrôle par des entreprises qui n'en sont qu'au début de leur projet sécuritaire. Les informations recueillies leur fourniront dans ce cas des bases pour structurer leurs capacités de cyberrésilience.

Vous devez, pour chacune des questions ci-dessous, choisir l'option qui reflète le mieux les pratiques actuelles de votre entreprise. À chacune des réponses proposées correspond une couleur, selon le principe suivant :

- Réponse la moins souhaitable : des améliorations doivent absolument être envisagées.
- Quelques améliorations pourraient être apportées afin de mieux protéger l'entreprise.
- La réponse dénote une excellente résilience face aux cybermenaces.

Les réponses au questionnaire reflètent le point de vue personnel de chaque interrogé, la *liste de contrôle plus précise associée à chaque question* est destinée à vous aider à identifier et à documenter un certain nombre de points de contrôle fondamentaux de sécurité de l'information de votre entreprise. Les informations recueillies au cours de ce processus devraient mettre en lumière les failles et les vulnérabilités des entreprises utilisant le présent guide, afin qu'elles sachent sur quels éléments faire porter leurs efforts.

1

Évaluez-vous la manière dont les informations sensibles sont traitées au sein de votre entreprise ?

✖ Non, mais nous avons un pare-feu pour nous protéger contre le vol d'informations.

! Oui, nous comprenons l'importance de nos informations et mettons en œuvre des mesures générales de sécurité.

✔ Oui, et nous disposons d'un modèle de classification de l'information et savons où nos données sensibles sont stockées et traitées. Nos mesures de sécurité sont établies en fonction du niveau de sensibilité des informations.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Vos données sensibles sont-elles identifiées et classifiées ?		
Êtes-vous conscient de vos responsabilités en ce qui concerne les informations identifiées comme sensibles ?		
Les données les plus sensibles sont-elles hautement protégées ou chiffrées ?		
Disposez-vous de procédures applicables à la gestion des données à caractère personnel ?		
Vos employés sont-ils tous capables d'identifier et de protéger adéquatement les données sensibles et non sensibles ?		

2

Effectuez-vous des analyses de risques en matière de sécurité de l'information ?

✖ Nous n'effectuons pas d'analyse de risques.

! Nous effectuons des analyses de risques, mais pas sur des sujets touchant spécifiquement à la sécurité de l'information.

✔ Nous effectuons des analyses de risquessur des sujets touchant spécifiquement à la sécurité de l'information.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Traitez-vous les vulnérabilités détectées par niveau de risque, du plus élevé au plus faible ?		
Les événements susceptibles d'entraîner des interruptions de l'activité de l'entreprise sont-ils identifiés, et l'impact de celles-ci est-il évalué ?		
Disposez-vous d'un plan de continuité d'activité régulièrement testé et mis à jour ?		
Effectuez-vous régulièrement des analyses de risquesafin de réévaluer le niveau de protection nécessaire de l'information et des données ?		
Les zones de risque de vos différents processus sont-elles identifiées de manière à empêcher la corruption ou l'utilisation malveillante de vos données ?		

3

À quel niveau la gouvernance de la sécurité de l'information se situe-t-elle dans votre organisation ?

✖ Il n'y a pas de gouvernance de la sécurité de l'information.

! La gouvernance de la sécurité de l'information est assurée par l'équipe informatique car c'est là que l'information a besoin d'être sécurisée.

✔ La gouvernance de la sécurité de l'information est assurée au niveau de l'équipe dirigeante, afin de veiller à ce que l'ensemble de l'entreprise soit concerné.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Les membres du conseil d'administration et le PDG allouent-ils un budget à la sécurité de l'information ?		
La sécurité de l'information fait-elle partie de la gestion du risque assurée par l'équipe dirigeante ?		
L'équipe dirigeante approuve-t-elle la politique de sécurité de l'information de l'entreprise, et la communique-t-elle correctement aux employés ?		
Les membres du conseil d'administration et l'équipe dirigeante sont-ils régulièrement informés des dernières évolutions des politiques, normes, procédures et lignes directrices en matière de sécurité de l'information ?		
Y a-t-il au moins un membre de l'équipe dirigeante qui soit chargé de la protection des données et de la vie privée ?		

4

Disposez-vous au sein de votre entreprise d'une équipe ou d'une fonction dédiées à la sécurité de l'information ?

✖ Nous n'avons pas d'équipe, ni de rôles ou de responsabilités dédiés à la sécurité de l'information

! Nous n'avons pas d'équipe, mais nous avons défini au sein de l'entreprise des rôles et des responsabilités dédiés à la sécurité de l'information.

✔ Nous avons une équipe ou une fonction dédiées à la sécurité de l'information.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Un spécialiste ou une équipe identifié dédié à la sécurité de l'information coordonnent-ils les compétences internes et assistent-ils l'équipe dirigeante dans son processus de prise de décision ?		
Le spécialiste ou l'équipe identifié dédié à la sécurité de l'information ont-ils la responsabilité d'évaluer et de mettre systématiquement à jour la politique de sécurité de l'information en fonction d'incidents ou de changements notables ?		
Le spécialiste ou l'équipe identifié dédié à la sécurité de l'information disposent-ils d'une visibilité et d'un soutien suffisants pour intervenir dans toute initiative liée à l'information au sein de l'entreprise ?		
Différents responsables sont-ils en charge de différents types de données ?		
La faisabilité et l'efficacité de votre politique de sécurité de l'information ainsi que la performance de votre équipe dédiée à la sécurité de l'information sont-elles régulièrement évaluées par un auditeur ou un organe indépendant ?		

5

Comment gérez-vous les cyberrisques liés aux fournisseurs qui ont accès à vos données sensibles ?

✖ Nous avons une relation de confiance mutuelle avec nos fournisseurs.

! Nous insérons dans certains de nos contrats des clauses relatives à la sécurité de l'information.

✔ Nous avons mis en place des processus de validation d'accès pour les fournisseurs ainsi que des directives spécifiques en matière de sécurité qui leur sont communiquées et qu'ils doivent signer.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Les sous-traitants et fournisseurs sont-ils identifiés par un badge muni d'une photo récente ?		
Avez-vous une politique de contrôle des antécédents de vos sous-traitants et fournisseurs ?		
L'accès à vos locaux et systèmes est-il automatiquement désactivé lorsqu'un sous-traitant ou un fournisseur a terminé sa mission ?		
En cas de perte ou de vol d'informations, vos fournisseurs savent-ils comment et à qui, au sein de votre entreprise, les signaler immédiatement ?		
Votre entreprise s'assure-t-elle que les fournisseurs maintiennent à jour leurs logiciels et applications en utilisant des correctifs de sécurité ?		
Des exigences de sécurité sont-elles clairement définies dans vos accords contractuels avec vos sous-traitants et fournisseurs ?		

6

Votre entreprise évalue-t-elle régulièrement sa sécurité des systèmes d'information ?

✖ Nous n'effectuons ni audits ni tests d'intrusion pour évaluer notre sécurité des systèmes d'information.

! Notre approche ne comprend pas systématiquement des audits de sécurité et / ou des tests de pénétration, mais nous en effectuons occasionnellement.

✔ Notre approche comprend systématiquement des audits de sécurité et / ou des tests d'intrusion afin d'évaluer notre sécurité des systèmes d'information.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Effectuez-vous régulièrement des tests, et gardez-vous la trace des menaces identifiées ?		
Disposez-vous de procédures afin d'évaluer les menaces humaines pesant sur vos systèmes d'information, telles que la malhonnêteté, l'ingénierie sociale et l'abus de confiance ?		
Votre entreprise exige-t-elle de ses fournisseurs de services informatiques des rapports d'audit de sécurité ?		
L'utilité de chaque type de données stockées est-elle également évaluée lors des audits de sécurité ?		
Auditez-vous vos procédures et processus de sécurité de l'information afin de vérifier leur conformité avec les autres politiques et normes établies au sein de votre entreprise ?		

7

Lors de l'introduction de nouvelles technologies, votre entreprise évalue-t-elle les cyberrisques potentiels ?

✖ La sécurité de l'information ne fait pas partie du processus de mise en œuvre de nouvelles technologies.

! La sécurité de l'information n'est qu'occasionnellement prise en compte lors de la mise en œuvre de nouvelles technologies.

✔ La sécurité de l'information fait partie du processus de mise en œuvre de nouvelles technologies.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Lorsque vous envisagez de mettre en œuvre de nouvelles technologies, évaluez-vous leur impact potentiel sur la politique de sécurité de l'information établie au sein de votre entreprise ?		
Disposez-vous de mesures de protection afin de réduire les risques liés à la mise en œuvre de nouvelles technologies ?		
Les processus de mise en œuvre de nouvelles technologies sont-ils documentés ?		
Lors de la mise en œuvre de nouvelles technologies, votre entreprise peut-elle se reposer sur des partenariats permettant une collaboration et un échange d'informations sur des questions de sécurité clés ?		
La politique de sécurité de l'information de votre entreprise est-elle souvent considérée comme un obstacle à l'innovation technologique ?		
Votre entreprise utilise-t-elle dans le développement de nouvelles technologies une méthodologie de développement sécurisé à l'échelle du cycle de vie ?		

8

Avez-vous mis en place une formation à la sécurité de l'information au sein de votre entreprise ?

✖ Nous faisons confiance à nos employés et nous ne pensons pas qu'un accompagnement en matière de sécurité de l'information constitue une valeur ajoutée.

! Seules nos équipes informatiques reçoivent une formation spécifique afin de sécuriser notre environnement informatique.

✔ Des sessions de sensibilisation à la sécurité de l'information sont régulièrement organisées à l'intention de tous nos employés.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Adaptez-vous le contenu de certaines sessions de sensibilisation à la sécurité de l'information au domaine d'activité de vos employés ?		
Apprenez-vous à vos employés à se montrer attentifs aux atteintes à la sécurité de l'information ?		
Votre entreprise dispose-t-elle de directives claires concernant le signalement par les utilisateurs de faiblesses des systèmes ou des services, ainsi que de menaces pesant sur eux ?		
Vos employés savent-ils comment gérer correctement les données des cartes de crédit et les informations à caractère personnel ?		
Les utilisateurs extérieurs (le cas échéant) reçoivent-ils également une formation à la sécurité de l'information et sont-ils régulièrement tenus au courant des évolutions de vos politiques et procédures organisationnelles ?		

9

Comment utilisez-vous les mots de passe au sein de votre entreprise ?

✖ Nous partageons nos mots de passe avec d'autres collègues et / ou il n'existe pas de politique concernant leur usage sécurisé ou leur changement régulier.

! Tous les employés, y compris l'équipe dirigeante, possèdent des mots de passe uniques, mais aucune règle n'est imposée concernant leur complexité. Les changer est facultatif, et non pas obligatoire.

✔ Tous les employés, y compris l'équipe dirigeante, possèdent un mot de passe personnel qui doit satisfaire à des exigences précises en matière de complexité et être régulièrement changé.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Avez-vous établi et mis en œuvre une politique généralement acceptée en matière de mots de passe pour toutes les ressources accessibles au sein de votre entreprise ?		
Êtes-vous assuré que tous les mots de passe de votre entreprise : • ne sont pas stockés dans des fichiers facilement accessibles • ne sont pas faibles, en blanc ou laissés par défaut • ne restent pas inchangés ou rarement changés, en particulier en ce qui concerne les appareils mobiles.		
Vous sentez-vous bien protégé contre un accès physique non autorisé à vos systèmes ?		
Les utilisateurs et les sous-traitants ont-ils conscience de leur responsabilité de protéger également les équipements laissés sans surveillance, notamment en fermant les sessions avant de quitter leur poste ?		
Les employés ont-ils été formés à reconnaître les tentatives d'ingénierie sociale visant à les inciter à divulguer des détails de sécurité, et savent-ils comment réagir à cette menace ?		

10

Disposez-vous d'une politique relative à la bonne utilisation de l'internet et des médias sociaux ?

✖ Non, nous n'avons aucune politique relative à la bonne utilisation de l'internet.

! Oui, cette politique est affichée en un lieu accessible à tous les employés, mais il ne leur a pas été demandé de la signer.

✔ Oui, notre politique relative à la bonne utilisation de l'internet fait partie des contrats de travail / est signée par tous les employés.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Existe-t-il des directives et des processus généraux à l'intention des employés en ce qui concerne la communication, y compris avec la presse et sur les médias sociaux ?		
Existe-t-il un processus disciplinaire pour les employés qui contreviennent aux directives de l'entreprise en matière de communication ?		
Une équipe ou un responsable de la communication identifié font-ils régulièrement des recherches sur l'internet afin d'évaluer la cyberréputation de l'entreprise et les risques qui y sont liés ?		
Votre entreprise a-t-elle évalué sa responsabilité au cas où des employés ou d'autres utilisateurs ou attaquants internes utiliseraient ses systèmes pour commettre des actes illégaux ?		
Votre entreprise a-t-elle pris des mesures pour empêcher tout employé ou autre utilisateur interne d'attaquer d'autres sites ?		

11

Votre entreprise pratique-t-elle des contrôles, des comptes rendus et un suivi sur les sujets touchant à la sécurité de l'information ?

✖ Nous ne pratiquons ni contrôle, ni compte rendu, ni suivi en ce qui concerne l'efficacité et la pertinence des mesures de sécurité mises en œuvre.

! Notre entreprise a mis en place des outils et des méthodes de contrôle, de compte rendu et de suivi de l'efficacité et de la pertinence de certaines des mesures de sécurité mises en œuvre.

✔ Notre entreprise a mis en place des outils et des méthodes de contrôle, de compte rendu et de suivi de l'efficacité et de la pertinence de toutes les mesures de sécurité mises en œuvre.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Les journaux et conclusions d'audit concernant les incidents sont-ils conservés, et des mesures sont-elles prises afin d'empêcher que ceux-ci se reproduisent ?		
Votre entreprise vérifie-t-elle sa conformité aux exigences légales et réglementaires (par exemple sur la protection de la vie privée) ?		
Avez-vous développé vos propres outils afin d'aider l'équipe dirigeante à évaluer l'état général de la sécurité et de permettre à votre entreprise d'améliorer sa capacité de réduction des risques potentiels ?		
Votre entreprise dispose-t-elle d'une feuille de route relative à la sécurité de l'information définissant notamment des objectifs, des indicateurs de progrès et d'éventuelles possibilités de collaboration ?		
Les comptes rendus des contrôles et les incidents sont-ils portés à la connaissance des autorités et d'autres groupes d'intérêts tels que des associations sectorielles ?		

12

Comment les systèmes sont-ils maintenus à jour au sein de votre entreprise ?

✖ Nous nous reposons pour la plupart de nos solutions sur la gestion automatique des correctifs proposée par le fournisseur.

! Nous installons systématiquement tous les mois des correctifs de sécurité.

✔ Nous disposons d'un processus de gestion des vulnérabilités et nous nous tenons en permanence informés de l'évolution de la situation (par ex. par un abonnement à un service d'alerte automatique signalant toute nouvelle vulnérabilité), et nous installons des correctifs en fonction des risques auxquels ils remédient.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Des scans de vulnérabilité sont-ils régulièrement effectués dans le cadre de votre programme de maintenance ?		
Les applicatifs sont-ils revus et testés après tout changement dans les systèmes d'exploitation ?		
Les utilisateurs peuvent-ils vérifier eux-mêmes que toutes les applications ont bien été mises à jour par des correctifs ?		
Les utilisateurs sont-ils conscients qu'ils doivent également maintenir à jour le système d'exploitation et les applications, y compris les logiciels de sécurité, de leurs appareils mobiles ?		
Les utilisateurs sont-ils formés à reconnaître les messages d'alerte légitimes tel que les demandes d'autorisation de mise à jour (à distinguer de fausses alertes antivirus) et à avertir dûment l'équipe de sécurité en cas d'événement malheureux ou suspect ?		

13

Les droits d'accès des utilisateurs aux applications et systèmes sont-ils régulièrement réexaminés ?

✖ Les droits d'accès aux applications et systèmes ne sont pas systématiquement réexaminés ou supprimés.

! Les droits d'accès aux applications et systèmes ne sont supprimés que lorsqu'un employé quitte l'entreprise.

✔ Une politique de contrôle de l'accès est en place, avec un réexamen régulier des droits d'accès des utilisateurs pour l'ensemble des applications et systèmes d'exploitation.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Existe-t-il au sein de votre entreprise des politiques et des procédures limitant l'accès aux locaux et aux systèmes d'information électroniques ?		
Votre entreprise se repose-t-elle sur une politique de protection de la vie privée détaillant les informations qu'elle collecte (par exemple concernant vos clients : adresses physiques, adresses électroniques, historique de navigation, etc.) et la façon dont elles sont exploitées ?		
Vos politiques et procédures précisent-elles les méthodes utilisées pour contrôler l'accès physique aux zones sécurisées, par exemple verrouillage des portes, systèmes de contrôle d'accès ou surveillance vidéo ?		
L'accès aux locaux et aux systèmes d'information est-il automatiquement désactivé lorsqu'un membre du personnel quitte l'entreprise ?		
Vos données sensibles sont-elles classifiées (hautement confidentiel, sensible, uniquement pour usage interne) et les utilisateurs autorisés à y accéder inventoriés ?		
Des processus ont-ils été élaborés afin de réguler l'accès à distance aux systèmes d'information électroniques de votre entreprise ?		

14

Vos employés peuvent-ils utiliser leurs appareils personnels tels que téléphones portables et tablettes pour stocker ou transférer des informations de l'entreprise ?

✖ Oui, nos employés peuvent stocker ou transférer des informations de l'entreprise sur leurs appareils personnels sans mesures de sécurité particulières.

! Il existe une politique interdisant l'utilisation d'appareils personnels pour stocker ou transférer des informations de l'entreprise, mais, techniquement, nos employés peuvent le faire sans mesures de sécurité particulières.

✔ Les appareils personnels ne peuvent servir à stocker ou transférer des informations de l'entreprise qu'après la mise en œuvre de mesures de sécurité sur l'appareil concerné et / ou moyennant l'utilisation d'une solution professionnelle.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Votre entreprise se repose-t-elle sur une politique bien acceptée concernant l'utilisation d'appareils personnels ?		
Les appareils mobiles sont-ils protégés contre des utilisateurs non autorisés ?		
Tous les appareils et connexions sont-ils en permanence identifiés sur le réseau ?		
Les données des appareils mobiles sont-elles chiffrées afin de protéger leur confidentialité et leur intégrité ?		
L'équipe dirigeante est-elle consciente du fait que l'entreprise reste responsable des données, même si chaque employé est responsable de son appareil personnel ?		

15

Votre entreprise a-t-elle pris des mesures pour prévenir la perte des informations stockées ?

✖ Nous ne disposons pas de processus de sauvegarde / disponibilité des données.

! Nous disposons d'un processus de sauvegarde / disponibilité des données, mais aucun test de récupération n'a été effectué.

✔ Nous disposons d'un processus de sauvegarde / disponibilité des données incluant des tests de récupération / résilience. Nous stockons des copies de nos sauvegardes sur un autre site sécurisé, ou nous utilisons d'autres solutions garantissant la disponibilité des données.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Avez-vous suffisamment d'employés capables d'effectuer des copies de sauvegarde et d'archive récupérables ?		
Vos équipements sont-ils protégés des coupures de courant par l'utilisation de sources d'électricité permanentes telles qu'alimentations multiples, onduleurs, générateurs électriques, etc. ?		
Les supports de sauvegarde sont-ils régulièrement testés afin de veiller à ce que vos données puissent être récupérées dans les délais impartis à la procédure de restauration ?		
Votre entreprise dispose-t-elle de procédures de signalement de la perte ou du vol d'équipements mobiles ?		
Vos employés savent-ils comment réagir en cas de suppression accidentelle de données, et comment récupérer l'information en cas de désastre ?		
Des mesures ont-elles été prises pour protéger la confidentialité et l'intégrité des copies de sauvegarde sur le site de stockage ?		

16

Votre entreprise est-elle prête à gérer un incident de sécurité de l'information ?

✖ Nous sommes à l'abri des incidents. Et s'il en survient, nos employés sont suffisamment compétents pour y faire face.

! Nous avons des procédures de gestion des incidents, mais elles ne sont pas adaptées au traitement des atteintes à la sécurité de l'information.

✔ Nous avons un processus dédié au traitement des incidents de sécurité de l'information, ainsi que les mécanismes de recours à la hiérarchie et de communication nécessaires. Nous nous efforçons de traiter les incidents aussi efficacement que possible et d'en tirer les leçons afin de mieux nous protéger à l'avenir.

Les questions ci-dessous constituent une liste de contrôle de base de la sécurité de l'information de votre entreprise, destinée à vous aider à évaluer votre degré d'avancement dans le processus.	OUI	NON
Votre processus couvre-t-il différents types d'incidents, pouvant aller du déni de service à la violation de confidentialité, etc., ainsi que les moyens d'y faire face ?		
Votre entreprise dispose-t-elle d'un plan de gestion de la communication en cas d'incident ?		
Savez-vous quelles sont les autorités à avertir en cas d'incident, et comment procéder à ce signalement ?		
Votre entreprise a-t-elle trié et identifié les coordonnées des personnes à contacter pour chaque type d'incident ?		
Vous reposez-vous sur un responsable interne de la communication pour les contacts avec les employés et leurs familles ?		
Avez-vous mis en place un processus permettant de tirer les leçons des incidents de sécurité de l'information et d'améliorer ainsi leur gestion ?		

RESSOURCES ET RÉFÉRENCES

Ce guide s'accompagne d'une annexe numérique répertoriant d'autres documents, dont des normes de conduite et des standards techniques. Accessible sur le site web www.iccwbo.org/cybersecurity, cette annexe comprend une liste de cadres, de ressources et de contacts mondiaux utiles, auxquels s'ajouteront au fil du temps les cadres locaux transmis par les comités nationaux et les membres d'ICC. Elle offre un instantané des ressources existantes à la date de publication de ce guide mais sera régulièrement enrichie et mise à jour.

www.iccwbo.org/cybersecurity

The ICC Cyber security guide is also online with a one-stop resource portal offering globally relevant and localized standards, practices and advice on matters relating to technical as well as functional aspects of information security.

The portal features:

- Downloads of the ICC Cyber security guide for business
- Translated and/or locally adapted versions of the guide
- Links to globally recognized good practices, standards and frameworks
- List of public bodies and organizations with a global reach that are active in the domain of cyber and information security
- Links to country-specific resources developed by companies, government agencies and other entities.

NOTES

NOTES

LA CHAMBRE DE COMMERCE INTERNATIONALE (ICC)

ICC est l'organisation mondiale des entreprises. Elle est l'unique porte-parole reconnu de la communauté économique à s'exprimer au nom de tous les secteurs et de toutes les régions.

ICC a pour mission d'encourager les échanges et les investissements internationaux et d'aider les entreprises à relever les défis et saisir les opportunités de la mondialisation. Depuis sa fondation, au début du XXe siècle, son action repose sur la conviction que le commerce est une puissante force de paix et de prospérité, et le petit groupe de patrons clairvoyants qui fut à l'origine de sa création se qualifiait lui-même de « marchands de paix ».

Les activités d'ICC relèvent principalement de trois domaines : élaboration de règles, règlement des différends et politique générale. Le fait que ses entreprises et associations membres soient directement engagées dans le commerce international lui confère un poids sans égal dans la mise en place de règles destinées à guider la bonne marche des affaires dans le monde. Bien que ne faisant appel qu'à l'autodiscipline, ces règles sont quotidiennement respectées dans des milliers de transactions et font partie intégrante de l'édifice du commerce international.

ICC offre également de nombreux services pratiques essentiels, au premier rang desquels figurent ceux de sa Cour internationale d'arbitrage, principale institution mondiale de règlement des litiges commerciaux. Autre pièce maîtresse du dispositif d'ICC, sa Fédération mondiale des chambres de commerce (WCF) a pour mission d'encourager la formation de réseaux et les échanges d'informations sur les pratiques d'excellence des chambres. ICC propose en outre des formations et des séminaires spécialisés et figure parmi les principaux éditeurs d'outils pratiques et pédagogiques dans le domaine du commerce international, de la banque et de l'arbitrage.

Cadres et experts des entreprises membres d'ICC travaillent à formuler le point de vue de la communauté économique internationale, tant sur de grands problèmes touchant au commerce et à l'investissement que sur des sujets techniques et sectoriels essentiels, dans le domaine, entre autres, de la lutte contre la corruption, de la banque, de l'économie numérique, de l'éthique du marketing, de l'environnement et de l'énergie, de la politique de la concurrence et de la propriété intellectuelle.

ICC entretient d'étroites relations de travail avec les Nations unies, l'Organisation mondiale du commerce et d'autres institutions intergouvernementales, dont le G20.

Fondée en 1919, ICC fédère aujourd'hui plus de 6 millions de sociétés, chambres de commerce et associations économiques, dans plus de 130 pays. Ses comités nationaux lui relaient les préoccupations de leurs adhérents et communiquent aux pouvoirs publics les avis qu'elle exprime au nom de la communauté économique mondiale.

CHAMBRE
DE COMMERCE
INTERNATIONALE

L'organisation mondiale des entreprises

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 **F** +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org

Publication number: 450/1081-5

ISBN: 978-92-842-0387-1