Principes de base pour la gestion des risques liés à la cybersécurité

En coopération avec le Centre pour la Cybersécurité Belgique.

Ce document est une communication de la FSMA faite en exécution de l'article 66 de la loi du 2 août 2002.

Ce guide est le résultat d'une coopération fructueuse avec le Centre pour la Cybersécurité Belgique.

La FSMA a consulté la Banque Nationale de Belgique et divers représentants spécialisés du secteur et elle tient à leur exprimer sa reconnaissance pour leur collaboration.

Avant-propos :

Les cybermenaces constituent un risque opérationnel majeur pour les entreprises actives dans le secteur financier. Elles méritent toute l'attention des entreprises puisque leurs clients, les données personnelles de ces clients ainsi que leur réputation sont leurs ressources (assets) les plus précieuses.

La FSMA souhaite sensibiliser et fournir des orientations sur les fondements de la gestion des cyberrisques en collaboration avec le Centre pour la Cybersécurité Belgique (ci-après aussi nommé « CCB »). Ce document contient des Principes de base en matière d'Information et de Cybersécurité afin d'aider toutes les entreprises à mettre en œuvre des mesures organisationnelles et techniques en matière de cybersécurité.

Les termes utilisés et liés au « cyber » dans le présent document ont le sens qui leur est donné dans le « Cyber Lexicon » du Conseil de stabilité financière (Financial Stability Board).

La FSMA attend de toutes les entreprises placées sous son contrôle[1] qu'elles adoptent les mesures nécessaires pour gérer les risques liés à la sécurité informatique et plus particulièrement les cyberrisques[2], compte tenu de la nature, de l'ampleur et de la complexité de leurs activités, en ce compris lorsqu'elles les sous-traitent. Ces mesures devraient être réévaluées et mises à jour régulièrement afin d'y intégrer les techniques et meilleures pratiques les plus récentes.

Le secteur financier est diversifié en termes de taille et de structure juridique des entreprises, allant des grandes entreprises aux entreprises unipersonnelles. La FSMA reconnaît que la pertinence et l'importance des questions soulevées dans le présent document varieront selon le modèle d'entreprise, la taille et la complexité technologique de l'entreprise. Par

---

1 ***Ce guide ne traite <u>pas</u> de la cyberrésilience des plateformes boursières ou de règlement d'importance systémique (qui doivent respecter des lignes directrices et exigences plus strictes), comme EURONEXT, ni des sociétés cotées dont l'information relève de la supervision de la FSMA.***

2 L'essentiel des définitions contenues dans ce document trouvent leur source dans le « Cyber Lexicon » publié par le Conseil de stabilité financière (12 novembre 2018) (ci-après, « le **Cyber Lexicon** »). Les termes utilisés et liés au « cyber » dans ce document ont le sens qui leur est donné dans le « Cyber Lexicon ». En cas de doute, il convient de se référer aux termes et définitions, en anglais, qui figurent dans le « Cyber Lexicon ». Les traductions de ces termes et définitions reprises dans le présent document sont des traductions libres.

Le Cyberrisque est défini comme la combinaison de la probabilité de survenue de cyberincidents et de leur impact.

Un Cyberincident est défini comme un événement cyber qui i) compromet la cybersécurité d'un système informatique ou des informations que le système traite, stocke ou transmet ; ou ii) viole les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, qu'il résulte d'une activité malveillante ou non.

conséquent, la profondeur et la portée des sujets abordés dans le présent document ne sont pas exhaustives.

Le présent document ne traite pas des conséquences, le cas échéant, d'une violation de la protection des données du point de vue du RGPD[3]. Toutes les entreprises doivent effectuer leur propre analyse au cas par cas.

La cybersécurité est un défi organisationnel, pas seulement un problème informatique.

La cybersécurité[4] est devenue un défi organisationnel que tout dirigeant d'entreprise doit comprendre. C'est un élément crucial de toute stratégie organisationnelle visant à sécuriser les ressources essentielles (assets) de l'entreprise. Les incidents en matière de cybersécurité peuvent provenir de l'intérieur ou de l'extérieur de l'entreprise. Ils peuvent être causés par des événements imprévisibles, une erreur humaine, ainsi qu'une intention malveillante (de l'intérieur ou de l'extérieur de l'entreprise).

Les courtiers en assurance belges spécialisés en cette matière estiment que les risques internes (comme l'erreur humaine) au sein des entreprises représentent 60 à 70 % des incidents de sécurité, tels que la divulgation non désirée de données à des personnes non autorisées, l'envoi de courriers avec de mauvaises pièces jointes, la publication par erreur de bases de données confidentielles, etc[5].

L'infrastructure informatique peut également être menacée par des dangers très ordinaires tels qu'un incendie, une inondation ou simplement la foudre qui frappe les bureaux d'une entreprise ; une entreprise peut aussi avoir sous-traité une partie de sa technologie informatique à des fournisseurs externes qui ne sont pas en mesure de fournir les services attendus ou qui ont eux-mêmes été victimes d'incidents de sécurité ou de cyberincidents.

Par ailleurs, la sophistication des cybermenaces externes continue d'évoluer. Le secteur financier est l'un des secteurs ayant le plus fait l'objet d'attaques[6]. Même des mesures de

---

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[4] **La Cybersécurité** est la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information et/ou des systèmes informatiques par le biais du cyberespace. En outre, d'autres qualités, telles que l'authenticité, la responsabilité, la non-répudiation et la fiabilité, peuvent également être concernées.

[5] Résultats d'une table ronde avec des courtiers en assurance spécialisés organisée par la FSMA en mai 2019 dans ses locaux.

[6] Selon l'analyse des données réalisée par IBM X-factor 2018, le secteur de la finance et de l'assurance a été le secteur le plus attaqué trois années de suite. Les « erreurs humaines » telles que les serveurs mal configurés, les bases de données cloud non sécurisées et les sauvegardes mal sécurisées (...) étaient responsables de 43 % des incidents d'information divulgués publiquement, ce qui représente une augmentation de plus de 20 % par rapport à l'année précédente.

cybersécurité solides peuvent être compromises lorsque, par exemple, un employé ouvre une pièce jointe d'un e-mail contenant un programme malveillant ou télécharge un logiciel malveillant sur les systèmes de l'entreprise. Les attaques courantes comprennent l'hameçonnage et le « spear phishing »[7], les logiciels malveillants et de rançon[8], ainsi que les virements frauduleux vers des tiers, qui impliquent fréquemment l'utilisation d'e-mails ou d'identifiants volés de clients ou de conseillers financiers.

Les incidents de cybersécurité, quelle que soit leur cause, peuvent être très dommageables pour une entreprise, au point de la mener à la faillite.

L'impossibilité de fournir des services financiers en raison d'un cyberincident est tout d'abord préjudiciable au public, mais aussi à la réputation et aux activités d'une entreprise – et éventuellement à la réputation du secteur financier.

Les entreprises sont-elles obligées de faire quelque chose ?

Toutes les entreprises sont légalement tenues de conserver les données relatives aux clients et aux transactions.

En outre, si une entreprise perd des données personnelles privées, elle est exposée à une responsabilité potentielle pour violation des lois sur la protection de la vie privée (RGPD)[9].

Dans le pire des cas, une négligence grave dans la gestion des données du client pourrait potentiellement constituer un acte criminel. Le dirigeant ou le chef d'entreprise pourrait voir sa responsabilité engagée, ce qui pourrait être une source de réclamations et de responsabilités financières importantes.

La FSMA rappelle à toutes les entreprises sous sa supervision qu'elles doivent se conformer à toutes les exigences légales ou réglementaires qui leurs sont applicables en matière de cybersécurité et de gestion des cyberrisques, ainsi qu'à toutes les exigences ou orientations

---

[7] **L'hameçonnage et les attaques de « *spear phishing* »** : L'hameçonnage est un terme plus large qui désigne tout stratagème visant à amener les victimes à partager des informations sensibles telles que des mots de passe, des identifiants ou des informations de carte de crédit pour des raisons malveillantes. Contrairement aux attaques de *spear phishing* (littéralement : harponnage), les attaques d'hameçonnage ne sont pas personnalisées à leurs victimes et sont généralement envoyées à un grand nombre de personnes en même temps (https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing).

[8] **Logiciel malveillant (*malware*)** : logiciel conçu dans une intention malveillante contenant des caractéristiques ou des capacités susceptibles de causer un préjudice direct ou indirect aux entités ou à leurs systèmes informatiques.

Ransomware : logiciel malveillant utilisé pour extorquer de l'argent à un utilisateur en bloquant son système informatique contre le paiement d'une rançon (souvent en cryptomonnaie).

[9] Par souci de clarté : le présent guide ne traite PAS des infractions à la réglementation du RGPD.

pertinentes définies au niveau européen ou international, par exemple par les Autorités européennes de surveillance (ESMA, EIOPA, EBA) ou par l'OICV (l'Organisation internationale des commissions de valeurs).

Ceci est tout particulièrement le cas pour les **entreprises qui sont légalement obligées de maintenir en tout temps une organisation adéquate.** Cette exigence implique l'établissement d'une stratégie et d'un cadre appropriés de gestion des cyberrisques, qui permettent à l'entreprise, entre autres, d'assurer la préservation des données et des fonctions essentielles et le maintien des services et des activités ou, lorsque cela n'est pas possible, la récupération rapide de ces données et fonctions et la reprise rapide de leurs services et activités.

La FSMA attend des conseils d'administration et de la haute direction de ces entreprises qu'ils prennent pleinement leurs responsabilités concernant les risques liés à la cybersécurité et qu'ils allouent une haute priorité à ces risques dans leur agenda. Les responsables doivent prendre les mesures appropriées et les plus récentes pour améliorer leur cyberrésilience[10] et s'attaquer énergiquement aux problèmes clés tels que l'alignement des stratégies informatique et commerciale, la sous-traitance des risques, la gestion du changement et la gestion de la cybersécurité.

Les entreprises légalement requises de maintenir une « organisation adéquate » doivent disposer des mesures, politiques et procédures organisationnelles et techniques appropriées pour assurer la cybersécurité et la cyberrésilience. Les entreprises qui sous-traitent des activités sujettes aux cyberrisques devraient s'assurer que le fournisseur de services auquel elles font appel dispose de mesures, politiques et procédures organisationnelles et techniques appropriées pour assurer la cybersécurité et la cyberrésilience des données, services et activités.

Bien entendu, les stratégies, cadres et/ou politiques qui ne se traduisent pas en actes n'auront aucun impact contre les cyberincidents tels que les virus informatiques ou les cyberattaques. Ces entreprises devraient donc également mettre au point des procédures pour réagir aux cybermenaces et se rétablir, et effectuer des tests adéquats sur la base de scénarios qui engagent le cœur de leur activité. Ces entreprises doivent considérer ce document comme une source d'inspiration utile, mais non exhaustive.

Les autres entreprises (qui ne sont pas tenues par la loi de maintenir une organisation adéquate, comme par exemple la plupart des intermédiaires financiers) devraient néanmoins adopter des mesures visant à protéger les données des consommateurs de services financiers, afin de contribuer au maintien d'un système et de services financiers solides et fiables pour le public.

[10] **La Cyberrésilience** est la capacité d'une organisation à poursuivre sa mission en anticipant et en s'adaptant aux cybermenaces et autres changements pertinents dans l'environnement, et en résistant aux cyberincidents, en les maîtrisant et en se rétablissant rapidement.

La FSMA encourage **toutes les entreprises** à accroître leur connaissance, ainsi que leurs mesures organisationnelles et techniques en matière de cybersécurité et à faire de cette question une priorité de la direction. Toutes les entreprises doivent s'assurer qu'elles comprennent et gèrent efficacement ces risques.

Ceci implique pour les entreprises de se poser des questions pour lesquelles elles chercheront de vraies solutions, avant de les tester en profondeur. À titre d'exemple, il est inutile d'avoir acheté un système de sauvegarde des données de l'entreprise lorsque la sauvegarde des données ne fonctionne pas dans la pratique...

Il convient également de clarifier la problématique avec les employés des entreprises. La cybersécurité concerne tous les employés et n'est pas une question technique réservée au spécialiste informatique.

Gestion de la cybersécurité : 4 principes clés

Pour établir une gestion efficace de la cybersécurité, quatre principes sont essentiels :

1. **Stratégie et soutien en matière de sécurité – Gouvernance**
   - Exiger la participation et le soutien de la direction.
   - Adopter une stratégie de sécurité de l'information (politique de sécurité) adaptée à la stratégie d'entreprise.
   - Mettre en place un plan pluriannuel de formation et de sensibilisation régulière pour l'ensemble du personnel.
   - Créer une culture de la sécurité de l'information et de l'analyse des risques pour tous les nouveaux projets.
   - Planifier la gestion d'incidents et de crises de sécurité majeurs ou graves.
   - Tenir un registre des changements majeurs dans l'environnement.
   - Disposer d'un Plan de réponse (*Cyber Incident Response Plan*).
2. **Identification des ressources (assets) et analyse des risques – Identification**
   - Identifier les systèmes informatiques et données clés.
   - Adopter une politique de catégorisation des systèmes informatiques et des données sensibles.
   - Gérer les risques liés à la sécurité informatique afin d'établir des priorités.
3. **Mise en œuvre de mesures – Protéger/détecter/répondre et rétablir**
   - Mettre en œuvre des mesures spécifiques (techniques/organisationnelles/processus) pour sécuriser l'information.

- Gérer les ressources affectées à la sécurité et à l'infrastructure informatique d'une manière efficace et rationnelle, y compris via la désignation d'agents de sécurité informatique.

4. Évaluation des mesures de sécurité

- Effectuer un examen au moins annuel des mesures de sécurité pour évaluer l'état du plan de sécurité.
- Mesurer à intervalles réguliers la performance des actions entreprises, mais aussi l'évolution des menaces et des vulnérabilités, afin d'assurer que les objectifs sont atteints (cycle d'amélioration continue).
- Envisager d'affiner l'analyse des risques et les mesures de contrôle à la lumière des évaluations, audits, incidents et changements majeurs, qui ont ou ont eu un impact sur les activités de l'entreprise.

1. Stratégie et soutien en matière de sécurité – Gouvernance

La gestion adéquate du cyberrisque est un problème d'entreprise, bien plus qu'un problème informatique technique. Une gestion efficace commence par un cadre clair et complet en matière de sécurité informatique et de cyberrésilience. Des dispositions doivent donc être prises pour établir, mettre en œuvre et revoir l'approche de l'entreprise en matière de gestion des cyberrisques.

La FSMA encourage **toutes les entreprises** à se doter d'un **Plan de réponse en cas de cyberincident (*Cyber Incident Response Plan*)**[11] qui indique de façon exhaustive les mesures à prendre pour protéger les données et reprendre les activités lorsqu'un incident survient.

La FSMA est d'avis que disposer d'un tel plan est indispensable pour les entreprises qui ont l'obligation légale de démontrer à tout moment un niveau d'organisation adéquat.

Ce Plan de réponse en cas de cyberincident doit accorder la priorité aux services fournis aux clients et prévoir toutes les mesures nécessaires pour permettre à l'entreprise de reprendre ses activités rapidement, en toute sécurité et avec des données exactes. Idéalement, le Plan s'articule autour des scénarios de catastrophe les plus courants et de ce qui nécessite le plus de protection. Il devrait également aborder la communication d'une manière adéquate et rapide avec toutes les parties prenantes concernées telles que, mais sans s'y limiter, les autorités judiciaires, les **Équipes d'intervention en cas de cyberincident (*Cyber Incident***

[11] **Plan de réponse en cas de cyberincident** : la documentation d'un ensemble prédéterminé d'instructions ou de procédures pour réagir aux conséquences d'un cyberincident et les limiter.

***Response Teams*)**[12] et, le cas échéant, l'Autorité de protection des données, les clients, etc. Un tel plan peut inclure le soutien de partenaires externes.

Les entreprises dotées de programmes de cybersécurité efficaces exigent généralement des employés qu'ils participent régulièrement à des formations et à des tests en matière de cybersécurité généraux et spécifiques à leur fonction, par exemple, par le biais d'exercices d'hameçonnage par e-mail.

Même si une entreprise a mis en place des bonnes pratiques, sa succursale ou ses bureaux de vente dispersés géographiquement doivent aussi faire l'objet d'attention, car ils ont peut-être plus de mal que le siège central à gérer les mots de passe, à installer des correctifs logiciel[13] et autres mises à jour, à mettre à jour les antivirus, à contrôler les périphériques de stockage amovibles (p. ex. clés USB), à chiffrer les données et à signaler les incidents.

Tous les points de vente doivent être formés pour faire face aux cyberincidents affectant l'entreprise : les clients poseront des questions au personnel de vente de l'entreprise et non au personnel informatique (qui sera de toute façon occupé à traiter le problème technique).

2. Identification des ressources (*assets*) et analyse des risques – Identification

Les entreprises déterminent celles de leurs opérations et ressources (*assets*) d'information de soutien essentielles (*critical operations and supporting information assets*) qui devraient, par ordre de priorité, être protégées contre toute compromission. L'établissement de l'inventaire est donc une première étape nécessaire et importante : quels sont les ressources (assets) ou processus les plus vitaux qui doivent être protégés ? Quelles sont les données les plus sensibles ?

Les entreprises dotées de programmes efficaces de sécurité informatique ou de cybersécurité établissent généralement de solides structures et processus de gouvernance (à l'échelle de l'entreprise) qui abordent la cybersécurité dans un contexte de gestion des risques. Elles transmettent les décisions et les problèmes liés à l'acceptation des risques aux niveaux appropriés pour qu'ils soient résolus – et partagent avec ceux-ci les informations concernant le développement futur des programmes.

---

[12] **Équipe d'intervention en cas de cyberincident** : équipe composée de membres de l'organisation compétents et dignes de confiance qui s'occupent des incidents pendant leur cycle de vie.

[13] **Gestion des correctifs :** les notification, identification, mise en œuvre, installation et vérification systématiques des révisions des codes des systèmes d'exploitation et des logiciels d'applications. Ces révisions sont connues sous le nom de correctifs, patchs (hot fixes) et packs de service.

Les mesures que ces entreprises mettent en œuvre peuvent comprendre des évaluations régulières des risques, ainsi que des plans de suivi détaillés aux délais précis, afin de résoudre les problèmes à plus haut risque. Les entreprises dotées de programmes de cybersécurité efficaces appuient généralement leurs évaluations des risques par des tests réguliers de vulnérabilité et de pénétration informatique[14].

Toutes les entreprises devraient garder à l'esprit que la proportionnalité est essentielle dans la mise en œuvre des processus et procédures de cybersécurité et doivent tenir compte de leur propre profil de risque – en se rappelant que le nombre d'employés n'est ni le seul indicateur de profil de risque, ni le plus pertinent.

3. Mise en œuvre de mesures – Protéger/détecter/répondre et rétablir

Toutes les entreprises devraient prendre des mesures adéquates pour protéger leurs clients et leurs données de transaction contre les violations externes et internes. Une répartition claire des responsabilités au sein de l'entreprise contribue dès lors à combler le fossé entre la théorie et la pratique. La détection précoce des infractions permettra aux entreprises de réagir rapidement et de prendre des contre-mesures face à une violation potentielle, voire de contenir une violation réelle.

En fonction de leur taille, certaines entreprises mettent en œuvre des solutions SIEM (gestion des événements et informations de sécurité), des outils d'analyse du « comportement d'utilisation du système » et des outils de prévention des pertes de données pour identifier, surveiller et traiter les activités potentiellement anormales ou suspectes sur leurs réseaux.

Les entreprises dépendent largement des fournisseurs de services informatiques pour le matériel et les logiciels. L'existence d'un processus officiel d'évaluation de l'état de préparation d'un fournisseur éventuel en matière de cybersécurité ou visant à s'assurer que les nouveaux fournisseurs ont mis en place les protections appropriées, constitue une bonne pratique.

Par exemple, le contrat d'une entreprise avec des fournisseurs devrait inclure des questions clés telles que les responsabilités des fournisseurs externes en matière de notification à l'entreprise dans le cas d'une violation des données des clients ou de l'entreprise. Si les services de cybersécurité sont fournis à plusieurs entreprises liées, les responsabilités en matière de cybersécurité doivent être suffisamment documentées dans l'intérêt de toutes les entreprises, par exemple dans un contrat de niveau de service (*service level agreement*).

[14] **Tests d'intrusion :** méthode de test dans laquelle les évaluateurs, en utilisant toute la documentation disponible (p. ex. conception du système, code source, manuels) et en travaillant sous des contraintes spécifiques, tentent de contourner les dispositifs de sécurité d'un système informatique.

4. Évaluation des mesures de sécurité

Toutes les entreprises devraient réévaluer leurs mesures de sécurité au moins une fois par an en mesurant l'efficacité des mesures prises. Une surveillance étroite et régulière des menaces et des vulnérabilités est nécessaire.

Toutes les entreprises doivent rester vigilantes face à l'évolution rapide des menaces et des vulnérabilités et se demander régulièrement si les mesures mises en œuvre sont à jour et suffisantes pour répondre aux objectifs de l'entreprise et à son appétit au risque.

Les entreprises disposant d'un Plan de réponse efficace en cas de cyberincident adoptent un **cycle d'amélioration continue** (*continuous improvement cycle*) consistant à affiner l'analyse des risques et des mesures de contrôle à la lumière des évaluations, audits, incidents et changements majeurs qui ont / ont eu un impact sur les activités commerciales, au moins sur une base annuelle.

Et pour une petite entreprise ?

Les petites entreprises qui éprouvent des difficultés à développer une stratégie et un cadre de gestion des cyberrisques peuvent s'inspirer du **Guide de référence de la cybersécurité** accessible en ligne et publié par le **Centre pour la Cybersécurité Belgique** (https://cyberguide.ccb.belgium.be).

Comme première étape de l'analyse de la situation en matière de cybersécurité, une petite entreprise peut souhaiter se poser les **Questions clés** jointes au présent document[15].

En cas de difficulté, une petite entreprise devrait demander de l'aide extérieure, en contactant des consultants ou des entreprises spécialisées, plutôt que d'attendre la survenue de problèmes.

Les compagnies d'assurance, auprès desquelles les entreprises peuvent demander une couverture d'assurance, peuvent également aider une entreprise à effectuer une analyse préventive de sa cyberrésilience afin d'évaluer le risque de l'entreprise.

Partager l'information

La FSMA encourage toutes les entreprises à partager leur expérience avec leurs pairs, par exemple par le biais de la page de contact de la **Cyber Security Coalition**[16] et de leur organisation professionnelle, car cela contribue à protéger le secteur financier et, par

[15] Ces questions sont issues du rapport final de la Cyber Task Force OICV-IOSCO (FR09/2019, juin 2019) (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf).

[16] www.cybersecuritycoalition.be

conséquent, à maintenir la confiance du public dans la capacité du secteur à protéger ses intérêts financiers.

La **loi du 7 avril 2019**[17] impose aux opérateurs de plateformes de négociation qualifiés en tant qu'opérateurs de services essentiels de signaler les incidents significatifs à la fois au Centre national de réponse aux incidents de sécurité informatique (National Computer Security Incident Response Team (CSIRT))[18] et à la FSMA. Les entreprises financières qui ont été identifiées comme opérateurs de services essentiels, autres que les opérateurs de plateformes de négociation, signalent les incidents significatifs à la Banque Nationale de Belgique, qui en informe à son tour le CSIRT[19].

Quelques références utiles :

Le Centre pour la Cybersécurité Belgique a publié un **Guide de référence de cybersécurité** accessible en ligne (https://cyberguide.ccb.belgium.be) qui contient des conseils pratiques, qui sont classés en deux catégories : les mesures de base et les mesures avancées.

Les entreprises peuvent trouver des lignes directrices plus élaborées (mises à jour de temps à autre) dans les documents suivants (étant entendu que les entreprises doivent dans ce cadre tenir compte du principe de proportionnalité et du statut juridique de l'entreprise concernée ainsi que de l'impact de ses activités sur les consommateurs de produits et services financiers ou sur la stabilité financière) :

1. Les rapports, orientations, recommandations, etc., publiés par des organismes internationaux (tels que l'OICV ou l'OCDE), par les Autorités européennes de surveillance (ESMA, EIOPA, EBA), par les banques centrales ou autorités nationales compétentes (telles que la Banque Nationale de Belgique) ou par des organismes disposant d'une expertise en matière de cybersécurité (tels que le Swift Institute).

Voir par exemple le Guide CPMI-OICV sur la Cyberrésilience des infrastructures des marchés financiers (www.bis.org/cpmi/publ/d146.pdf), ainsi que le rapport final de la Cyber Task Force OICV-IOSCO (juin 2019) (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf), le Cadre pour l'amélioration de la cybersécurité des infrastructures critiques (*Framework for Improving Critical Infrastructure Cybersecurity*) du NIST (National Institute of Standards and Technology) (https://www.nist.gov/cyberframework) et le toolkit publié en juillet 2019 par le Swift Institute (*Cyber Resilience and Financial Organizations: A Capacity-building Tool B*ox - https://swiftinstitute.org/research/securing-the-long-tail-of-financial-services-toolkit/).

---

[17] Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

[18] À la date de publication du présent document, le CSIRT doit être créé par un futur arrêté royal.

[19] Voir l'article 26 de la loi du 7 avril 2019.

2. La **loi du 7 avril 2019** établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, applique en Belgique la directive NIS[20], en ce qui concerne le partage des informations et la notification des incidents[21].

3. La **famille de normes ISO 27000 sur les systèmes de gestion de sécurité de l'information** publiées par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (IEC) (voir, par exemple, ISO, « ISO/IEC 27000:2018 », février 2018, https://www.iso.org/standard/73906.html).

4. Les informations régulièrement mises à jour sur la cybercriminalité de l'Équipe d'intervention d'urgence informatique de l'UE (Computer Emergency Response Team ou CERT-EU) (https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html).

5. Les documents et informations publiés par le **Centre pour la Cybersécurité Belgique** (https://www.ccb.belgium.be/fr) et la **Coalition belge pour la cybersécurité** (https://www.cybersecuritycoalition.be/).

6. Les principes fondamentaux du **G7** en matière de cybersécurité pour le secteur financier (*G-7 Fundamental elements for third party cyber risk management in the financial sector*) (https://fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf) et les principes fondamentaux du G7 pour les tests de pénétration

---

[20] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 5 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS) **:** https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. La directive NIS prévoit des mesures juridiques visant à renforcer le niveau global de cybersécurité dans l'Union européenne en assurant :

- La préparation des États membres en exigeant qu'ils soient équipés de manière appropriée, par exemple via un centre de réponse aux incidents de sécurité informatique (CSIRT) et d'une autorité nationale compétente NIS ;
- La coopération entre tous les États membres, via la création d'un groupe de coopération, afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres. Ils devront également mettre en place un réseau CSIRT, afin de promouvoir une coopération opérationnelle rapide et efficace sur les incidents de cybersécurité spécifiques et d'échanger des informations sur les risques ;
- Une culture de la sécurité dans tous les secteurs qui sont vitaux pour notre économie et notre société et qui, en outre, dépendent largement des TIC, tels que l'énergie, le transport, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé et les infrastructures numériques. Les entreprises de ces secteurs, identifiées par les États membres comme prestataires de services essentiels, devront prendre les mesures de sécurité appropriées et notifier les incidents graves aux autorités nationales compétentes. Les principaux fournisseurs de services numériques (moteurs de recherche, services informatiques en cloud et marchés en ligne) devront également se conformer aux exigences de sécurité et de notification prévues par la nouvelle directive.

[21] Voir article 4, § 3 de la loi du 7 avril 2019.

fondés sur les menaces (*G-7 Fundamental elements for threat-led penetration testing*) (https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf).

Terminologie

La normalisation est limitée concernant les mots liés au « cyber » et d'autres définitions peuvent donc être trouvées dans d'autres sources.

La majorité des définitions contenues dans le présent document trouvent leur source dans le **« Cyber Lexicon »** publié par le **Conseil de stabilité financière** (Financial Stability Board) daté au 12 novembre 2018 ; de même, les mots utilisés et liés au « cyber » dans le présent Guide ont le sens défini dans le Cyber Lexicon, sauf indication contraire expresse (https://www.fsb.org/2018/11/cyber-lexicon).

Les principaux termes utilisés dans le présent document :

Cyberrisque (*Cyber Risk*)	La combinaison de la probabilité de survenue de cyberincidents et de leur impact.
Cyberincidents (*Cyber Incident*)	Sont définis comme « des événements cyber qui i) compromettent la cybersécurité d'un système informatique ou des informations que le système traite, stocke ou transmet ; ou ii) violent les politiques de sécurité, les procédures de sécurité ou les politiques d'utilisation acceptable, qu'elles résultent d'une activité malveillante ou non ».
Plan d'intervention en cas de cyberincident (*Cyber Incident Response Plan*)	La documentation d'un ensemble prédéterminé d'instructions ou de procédures pour réagir aux conséquences d'un cyberincident et les limiter.
Équipe d'intervention en cas d'incident (*Incident Response Team*)	Une équipe de membres de l'organisation compétents et dignes de confiance qui s'occupent des incidents pendant leur cycle de vie.
Cyberrésilience (*Cyber Resilience*)	La capacité d'une organisation à poursuivre sa mission en anticipant et en s'adaptant aux cybermenaces et autres changements pertinents dans l'environnement, et en résistant aux cyberincidents, en les maîtrisant et en se rétablissant rapidement.

Équipe d'intervention en cas de cyberincident (Cyber *Incident Response Team*)	Équipe de membres de l'organisation compétents et dignes de confiance qui s'occupent des incidents pendant leur cycle de vie.
Logiciel de rançon ou malveillant (*Ransomware/Malware*)	Logiciel conçu dans une intention malveillante contenant des caractéristiques ou des capacités susceptibles de causer un préjudice direct ou indirect aux entités ou à leurs systèmes informatiques.
Gestion des correctifs (*Patch Management*)	Les notification, identification, mise en œuvre, installation et vérification systématiques des révisions des codes des systèmes d'exploitation et des logiciels d'applications. Ces révisions sont connues sous le nom de correctifs, patches, hot fixes et packs de service.
Test d'intrusion (*Penetration Testing*)	Méthode de test dans laquelle les évaluateurs, en utilisant toute la documentation disponible (p. ex. conception du système, code source, manuels) et en travaillant sous des contraintes spécifiques, tentent de contourner les dispositifs de sécurité d'un système informatique.

QUESTIONS CLÉS

Source : Final Report Cyber Task Force OICV-IOSCO Juin 2019
(https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf)[22]

Comme première étape de l'analyse de sa situation en matière de cybersécurité, une entreprise pourrait se poser les questions suivantes :

A. CADRE STANDARD DE L'INDUSTRIE :

1. *L'entreprise utilise-t-elle une norme de l'industrie pour élaborer une stratégie et un cadre de gestion des cyberrisques (p. ex. ISO, Cadre pour la cybersécurité du NIST ou autres) ? Veuillez identifier la ou les normes.*

B. IDENTIFIER ET PROTÉGER :

2. *L'entreprise tient-elle un inventaire de ses logiciels, matériels, applications et fournisseurs ?*

[22] Traduction officieuse.

3. *L'entreprise identifie-t-elle les cyberrisques et les vulnérabilités qui peuvent avoir un impact sur les activités commerciales ?*
4. *L'entreprise dispose-t-elle d'un programme de gestion de l'identification et de l'accès conçu pour limiter et retirer l'accès à ses utilisateurs en temps opportun ?*
5. L'entreprise dispose-t-elle d'un programme de sensibilisation et de formation à la sécurité qui permet aux individus de comprendre leur rôle concernant la cybersécurité et d'en apprendre davantage sur les nouvelles menaces ?
6. L'entreprise utilise-t-elle un programme de gestion des correctifs pour corriger les vulnérabilités logicielles connues ? L'entreprise utilise-t-elle du matériel (p. ex. pare-feu, systèmes de détection d'intrusion dans le réseau) et des logiciels (p. ex. anti-malwares, systèmes de détection d'intrusion de l'hôte) pour protéger ses systèmes informatiques ?
7. L'entreprise dispose-t-elle de procédures écrites pour s'assurer que des sauvegardes de l'information sont effectuées, conservées et testées périodiquement ?

C. DÉTECTER :

8. L'entreprise détecte-t-elle et analyse-t-elle les cyberévénements potentiels pour comprendre la nature, la portée et les méthodes d'une menace ?
9. L'entreprise met-elle en œuvre des mécanismes de protection des e-mails pour analyser, détecter et bloquer automatiquement les logiciels malveillants ou les liens malveillants dans les messages électroniques ?
10. L'entreprise dispose-t-elle d'un programme d'essais pour valider l'efficacité de ses processus et contrôles de détection des incidents ?

D. RÉPONDRE/RÉTABLIR :

11. L'entreprise dispose-t-elle d'un plan de réponse en cas d'incident pour contenir les cyberincidents ; et d'applications et de processus pour assurer l'alerte et l'activation du plan ?
12. Le plan de réponse en cas d'incident de l'entreprise traite-t-il du partage de l'information, y compris la gestion des divulgations de vulnérabilités et d'autres communications, et le signalement des cyberincidents aux parties prenantes internes et externes, aux tiers, aux organismes de réglementation et d'application de la loi, le cas échéant ?
13. L'entreprise teste-t-elle régulièrement son plan de réponse en cas d'incident et le met-elle à jour, si nécessaire, en fonction des cyberincidents qui se sont produits et des renseignements sur les menaces ?
14. L'entreprise dispose-t-elle d'un plan de rétablissement pour assurer un rétablissement rapide des activités à la suite de cyberincidents ?
15. L'entreprise révise-t-elle et met-elle à jour périodiquement son plan de rétablissement ?