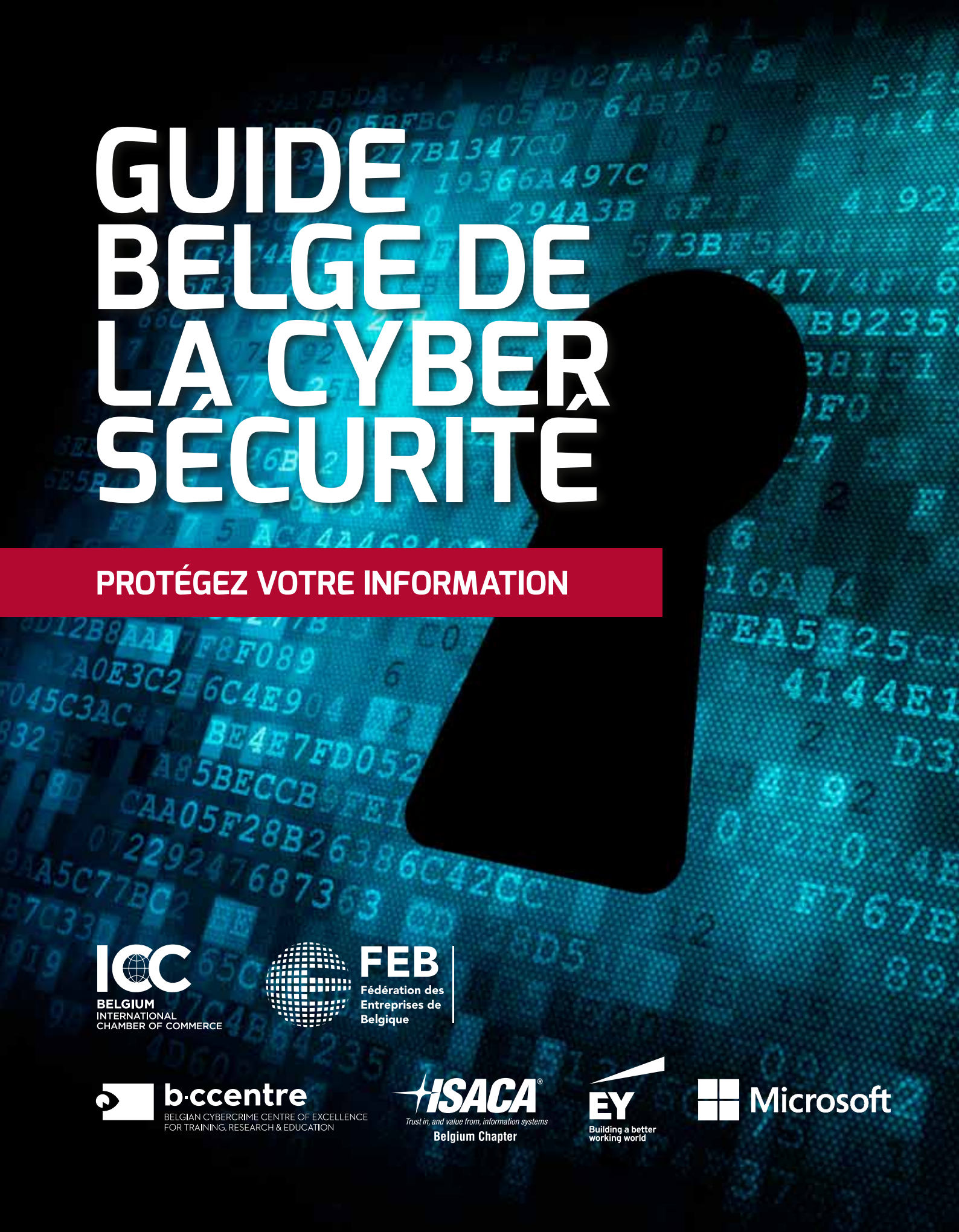


GUIDE BELGE DE LA CYBER SÉCURITÉ

PROTÉGEZ VOTRE INFORMATION

BELGIUM INTERNATIONAL CHAMBER OF COMMERCE

FEB
Fédération des Entreprises de Belgique

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION

ISACA®
Trust in, and value from, information systems
Belgium Chapter

EY
Building a better working world

Microsoft

Le présent guide et les documents qui l'accompagnent ont été élaborés conjointement par ICC Belgium, la FEB, EY, Microsoft, L-SEC, le B-CCENTRE et ISACA Belgium.

L'objectif n'est pas de constituer un guide exhaustif des cyber-menaces potentielles ou de leurs mesures d'atténuation.

Les informations fournies :

- sont exclusivement de nature générale et ne s'adressent pas à une situation spécifique ni à des personnes physiques ou morales ou à des entités juridiques en particulier ;
- ne sont pas nécessairement complètes, précises ou à jour ;
- ne constituent pas un conseil professionnel ou légal ;
- ne remplacent pas un conseil d'expert ;
- ne fournissent aucune garantie d'une protection sûre.

AVANT-PROPOS

LA CYBER-SECURITE ...
ESSENTIELLE POUR TOUTE ENTREPRISE

Cher lecteur,

Par cette brochure, notre objectif est de vous familiariser davantage avec un sujet d'une importance majeure, régulièrement sous le feu des projecteurs : la sécurité de l'information.

Chaque jour, toutes sortes de cas de cyber-criminalité ou cyber-infractions surviennent tout autour du globe. Beaucoup les ignorent ou préfèrent les cacher, mais pour certaines entreprises, elles constituent une source de préoccupation considérable. Plusieurs incidents graves de cyber-sécurité ont ainsi eu lieu dernièrement dans notre propre pays. Il est aussi devenu de plus en plus évident que plusieurs gouvernements étrangers sont prêts à investir massivement dans la collecte d'informations. Et pourtant, ni l'ignorance, ni la négligence, ni la panique ne sont des réponses adéquates lorsqu'il s'agit de faire face au phénomène du cyber-crime.

En affaires, nous devons saisir les opportunités qui se présentent, et savoir gérer les risques avec sagesse. Chaque entrepreneur ou manager sait quelles connaissances, quelles technologies ou quels processus rendent son entreprise solide ou même unique, mais aussi vulnérable. Ce sont tout particulièrement ces actifs qui doivent être protégés par une bonne gouvernance en matière de sécurité de l'information. Une telle gouvernance aide à protéger l'entreprise des lourds dommages qui peuvent découler de mauvaises habitudes ou d'une relative négligence en matière de sécurité - lesquelles semblent d'ailleurs aller de pair avec le déferlement des médias sociaux, appareils mobiles et apps toujours plus personnalisés.

Laissez votre intérêt pour une meilleure protection vous guider vers une nouvelle dimension dans votre culture d'entreprise, et vers l'émergence d'une nouvelle compétence professionnelle : l'acquisition d'un réflexe 'cyber-sécurité' dans un environnement en perpétuelle évolution.

La présente brochure vous présente les principes clés en matière de cyber-sécurité et fournit une checklist simple, conçue pour vous permettre de vous lancer dans la bonne direction et mettre facilement en œuvre les conseils prodigués.

Nous espérons que ce guide sera utile à tous les responsables d'entreprises de notre pays.

Rudi Thomaes
Secrétaire Général d'ICC Belgium

Philippe Lambrecht
Secrétaire Général de la FEB

TABLE DES MATIERES

POURQUOI AVONS-NOUS BESOIN D'UN GUIDE DE LA CYBER-SÉCURITÉ ?

CETTE RUBRIQUE N'A PAS POUR BUT DE VOUS EFFRAYER, ET POURTANT ...

Les risques de sécurité augmentent.

Chaque jour, que ce soit au niveau personnel ou au niveau d'une entreprise, nous sommes exposés à des menaces en provenance du cyber-espace. Dans la plupart des cas, nous n'avons même pas conscience de ces menaces, ou si nous les connaissons, nous n'y apportons pas la réaction adéquate.

Les médias ne cessent de rapporter de nouveaux incidents relatifs à la sécurité, relatant l'impact qu'ils ont sur nous, personnes ou entreprises. Et pourtant, ces incidents ne sont que la partie émergée de l'iceberg : nous sommes bien plus exposés que nous l'imaginons, et les menaces sur internet se démultiplient à une vitesse impressionnante.

Le risque en matière de sécurité de l'information peut être vu comme la combinaison de trois facteurs : un actif, une vulnérabilité et une menace. Le principe est simple : un actif peut avoir des vulnérabilités, lesquelles peuvent être exploitées par des menaces. **Or, les faits sont là : ces trois facteurs ont connu une importante recrudescence au cours des dernières années :**

1. L'information[1] est un actif important de l'entreprise, et nous n'avons jamais géré de telles quantités d'informations au format électronique. Cela rend toujours plus forte notre dépendance aux systèmes qui traitent et stockent nos données. Or, qui dit bon fonctionnement, dit fonctionnement sûr : la sécurité de nos informations et de nos systèmes est donc critique.
2. De nouvelles techniques émergent et viennent compléter notre paysage technologique : le cloud computing, les médias sociaux, les appareils mobiles, pour n'en citer que quelques-uns. Cette évolution vers toujours plus de technologie va se poursuivre, et va continuer à accroître notre dépendance à leur bon fonctionnement. Mais chacune de ces technologies amène également de nouvelles vulnérabilités en matière de sécurité, que les entreprises ne sont pas toujours prêtes à affronter.
3. Enfin et surtout, le nombre de cyber-menaces a lourdement augmenté. La sophistication de ces menaces et leur efficacité a également connu une croissance inquiétante.

Alors, que de mauvaises nouvelles ? Pas vraiment. Mais quand même.

La bonne nouvelle, c'est qu'au cours des dernières années, nous avons assisté à une meilleure prise de conscience du problème, menant à diverses contre-mesures. Une série de bonnes initiatives ont déjà été lancées au niveau gouvernemental et institutionnel, mais elles n'ont peut-être pas encore été suffisamment adoptées dans le monde des entreprises.

En effet, il règne encore beaucoup d'incertitude quant à "ce qu'il faut faire" et "comment le faire", quand il s'agit de gérer les risques émanant des cyber-menaces. En règle générale, davantage d'initiatives sont prises dans des entreprises internationales de taille plus importante, alors que les entreprises moyennes ou familiales sont tout autant exposées à ces menaces. Et même dans les plus grandes entreprises, les initiatives en matière de sécurité de l'information ne font souvent pas l'objet d'un engagement fort de la part du plus haut niveau de l'entreprise. Nous sommes cependant convaincus que la sécurité de l'information devrait être à l'ordre du jour dans toutes les organisations - indépendamment de leur taille, de la complexité ou de la nature de leurs activités – et s'adresser à chaque individu qui les compose. Beaucoup d'entreprises protègent parfaitement leurs actifs physiques – installations, machines, personnel.

C'est la plupart du temps une question de bon sens et même d'habitude que d'assurer leur sécurité physique, de définir des règles de sécurité, de prévention et de protection dans les opérations de l'entreprise. Pourtant, l'information est également un bien précieux : son vol, sa perte, son mauvais usage, sa modification ou sa diffusion sans autorisation, peuvent tous avoir un impact et des conséquences graves. Le savoir-faire et les données de l'entreprise sont souvent parmi ses actifs les plus critiques. Assurer la confidentialité, l'intégrité et la disponibilité de ces données est devenu une priorité. Ces trois objectifs en matière de sécurité correspondent à trois questions clés : *"Qui consulte nos données ?", "Nos données ont-elles été corrompues ?" et "Pouvons-nous accéder à nos données quand nous en avons besoin ?".*

Il en va aussi de votre responsabilité.

On ne s'attend pas à ce que des dirigeants d'entreprises se convertissent en experts en cyber-sécurité. Toutefois, il est de leur devoir de protéger les actifs de leur organisation. Ils devront donc en déléguer la responsabilité à leurs équipes de direction et à des experts externes, afin de s'assurer que la cyber-sécurité reste un sujet régulièrement suivi par le conseil d'administration, et que les actions nécessaires soient entreprises.
Traiter des données personnelles au format électronique implique de nombreuses obligations pour une entreprise. En effet, elle est responsable des données qu'elle gère, et doit par conséquent assurer un niveau de sécurité adéquat. Il revient donc à chaque entreprise de prendre les mesures les plus pertinentes afin de protéger ces données contre une perte volontaire ou accidentelle, et empêcher leur utilisation ou modification non autorisée.

En plus d'autres sanctions que l'entreprise peut encourir, la loi prévoit des mesures pénales. Le projet de règlement européen sur la protection des données augmentera la sévérité de ces mesures et l'entreprise pourrait être contrainte à payer des dommages considérables aux personnes touchées.
En vertu du projet de règlement européen sur la protection des données, en cas de mauvais usage par des tiers des données personnelles détenues par l'entreprise, de perte de données ou de toute autre violation de celles-ci, l'entreprise doit en informer sans délai la commission de protection de la vie privée, ainsi que la personne concernée lorsque la violation des données est susceptible d'avoir un effet négatif sur la vie privée.

Il est temps d'agir !

Être la victime d'un incident en matière de sécurité de l'information peut avoir de multiples conséquences, ne se limitant pas à la perte de données ou d'informations. Les effets sur la réputation de votre entreprise peuvent perdurer et avoir de graves conséquences financières. Affirmer que protéger les informations de l'entreprise relève de la responsabilité de chacun ne suffit pas. Il faut rendre ce principe tangible à tous les niveaux de votre entreprise et ancrer des réflexes de sécurité dans le quotidien de vos équipes. Ces principes doivent être empreints de bon sens et être pragmatiques, afin de renforcer leur impact et de permettre une mise en œuvre tant dans les grandes que les petites entreprises – il convient donc d'éviter une approche unique qui ne tiendrait pas compte des spécificités de chaque organisation.

Une gouvernance professionnelle de la sécurité de l'information revient à

(A) créer une vision d'entreprise et des principes en la matière, lesquels devraient se traduire en une politique de sécurité de l'information,
(B) insérer cette politique dans l'organisation et établir les processus, rôles et responsabilités liés,
(C) créer la bonne culture, le bon comportement et les bons réflexes en mettant en œuvre de bonnes pratiques en matière de sécurité de l'information.

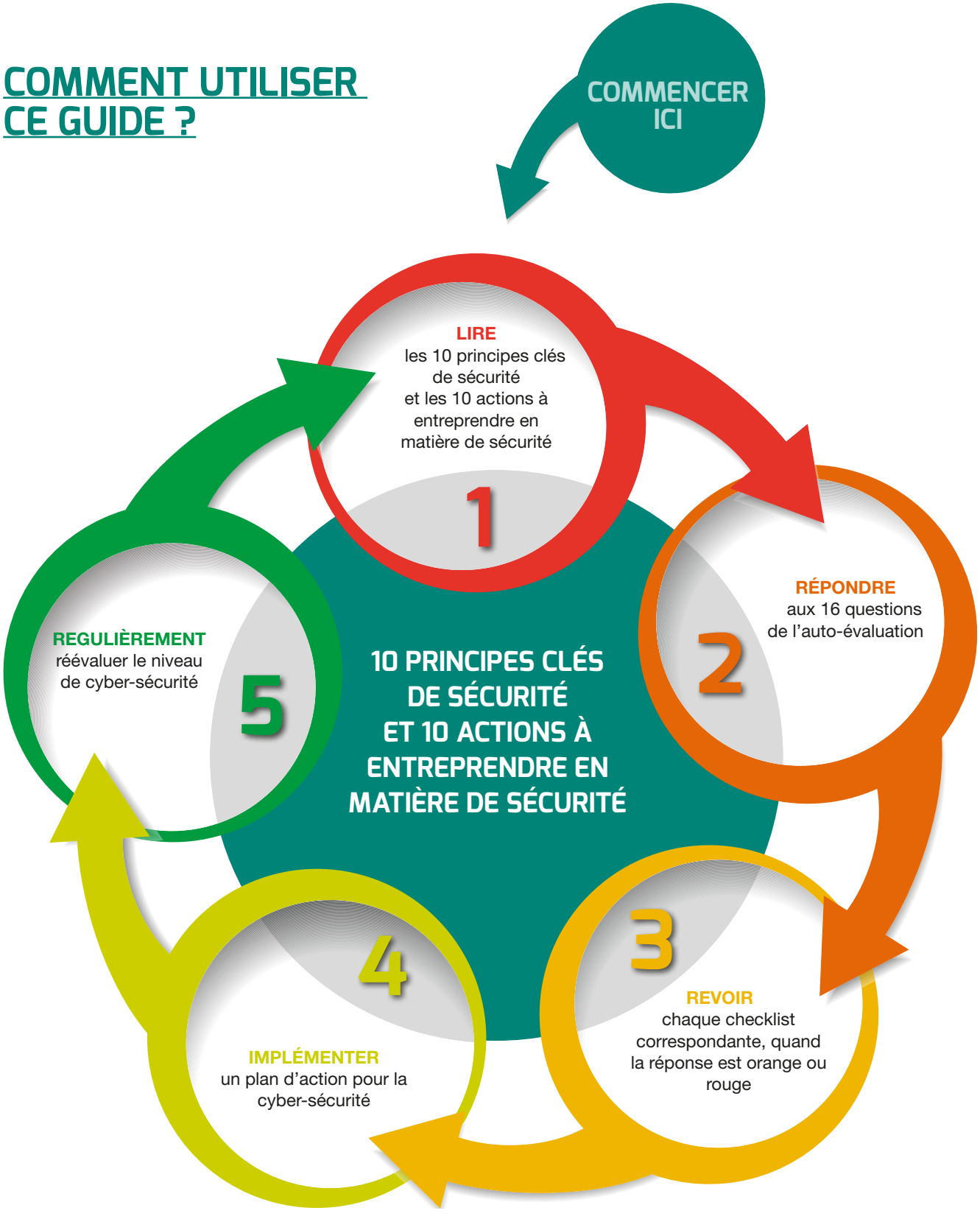
Cette combinaison doit permettre à votre entreprise d'atteindre des résultats durables dans le cadre de la sécurité de l'information. Une responsabilisation de chacun et une discipline rigoureuse, plutôt que des technologies de protection sophistiquées, sont des actions simples qui ont pourtant le potentiel d'améliorer considérablement votre niveau de cyber-sécurité.

La sécurité absolue est une utopie, mais cela ne devrait pas nous empêcher d'essayer de l'atteindre. Ce guide, écrit pas des représentants du monde de l'entreprise, devrait vous permettre d'entamer votre trajet vers une sécurité de l'information plus forte et plus durable.

[1] Citons notamment parmi les informations cruciales d'une entreprise : les données financières, les données RH, les données relatives aux clients et aux fournisseurs, les listes de prix, les comptes rendus du conseil d'administration ...

COMMENT UTILISER CE GUIDE ?

COMMENT UTILISER CE GUIDE ?



A. LA VISION

B. L'ORGANISATION & LES PROCESSUS

C. LA CULTURE D'ENTREPRISE

10 PRINCIPES CLÉS DE SÉCURITÉ

Il existe un certain nombre de principes-clés qui constituent la base d'une gestion efficace de la sécurité de l'information. Si l'approche pratique de gestion de la cyber-sécurité peut varier d'une entreprise à l'autre - suivant la nature de l'activité, le niveau de risque, les facteurs environnementaux, les exigences réglementaires, la taille - ces 10 principes s'appliquent à toutes les entreprises, quels qu'en soient la taille ou le secteur.

Ce guide présente **10 principes clés** structurés autour de trois domaines de la gouvernance de la sécurité de l'information :

(A) La vision

(B) L'organisation & les processus

(C) La culture d'entreprise

complétés par une série **d'actions à entreprendre en matière de sécurité.**

Les principes et les actions suggérés dans le présent guide renforceront considérablement la capacité de résistance d'une entreprise aux cyber-attaques, et en limiteront l'impact en cas d'incident.

1.

— ALLER AU-DELÀ DE LA TECHNOLOGIE —

Voir plus loin que la technologie, c'est envisager la sécurité de l'information dans son sens le plus large, et pas uniquement en termes de technologies de l'information (IT).

L'expérience[2] nous montre que 35% des incidents sont dus à une erreur humaine, plutôt qu'à une attaque délibérée. Et si l'on s'intéresse aux 65% restants, plus de la moitié de ces attaques délibérées auraient échoué si les individus impliqués avaient traité l'information de manière plus sécurisée.

Ces chiffres démontrent clairement que la gestion de la sécurité doit être vue comme une combinaison de personnes, de processus et de technologie. La cyber-sécurité doit être perçue comme l'affaire de toute l'entreprise, et pas seulement de l'informatique. La mise en œuvre de mesures de sécurité ne doit pas être limitée au département IT : elle doit être répercutée dans toute l'organisation, et se refléter dans chacune de ses actions. Le périmètre de la cyber-sécurité doit donc couvrir les personnes, les produits, les installations, les processus, les politiques de l'entreprise, les procédures, les systèmes, les technologies, les réseaux et l'information.

Dans une entreprise mature, la sécurité de l'information est considérée comme une exigence métier, alignée sur les objectifs stratégiques, les politiques de l'organisation, la gestion du risque, les exigences de conformité et la mesure des performances. Les dirigeants au sein de votre entreprise doivent pouvoir comprendre comment la sécurité sert l'entreprise.

Citons parmi les avantages de voir plus loin que la technologie, et de mettre la sécurité au service de l'entreprise:

- **Stratégiquement :** une meilleure prise de décision grâce à une visibilité plus forte sur l'exposition aux risques.
- **Financièrement :** une réduction des pertes, donnant un avantage financier à l'entreprise.
- **Opérationnellement :** l'existence de plans de contingence adéquats pour l'entreprise.

[2] EY – 2012 Global Information Security Survey - Fighting to close the gap (Enquête mondiale sur la sécurité de l'information de EY)

2.

— ALLER AU-DELÀ DE LA CONFORMITÉ —

Les entreprises sont soumises à de nombreuses lois, réglementations et normes, dont beaucoup requièrent la mise en place de mesures de sécurité adéquates. Le législateur et les régulateurs s'intéressent de près aux questions de la vie privée, des contrôles sur l'établissement des comptes de l'entreprise, de la protection du consommateur ou d'autres données spécifiques. Les textes légaux qui en découlent sont souvent complétés par des réglementations propres au secteur ou des cadres de sécurité.

La conformité avec ces diverses sources d'obligations a certes élevé le niveau de cyber-sécurité des entreprises. Toutefois, les efforts consentis n'ont trop souvent que la mise en conformité pour objectif.

La conformité étant toujours concentrée sur des sujets bien spécifiques, on dénote l'absence d'une approche globale, qui se fonde sur les risques réellement encourus.

Par exemple, les efforts de protection de la vie privée se concentrent uniquement sur la protection des données personnelles, et pas sur d'autres données, même si celles-ci sont tout aussi critiques. Le contrôle sur les états financiers se concentrera essentiellement sur l'intégrité des données financières, alors que d'autres informations gérées par l'entreprise pourraient faire l'objet des mêmes mesures de protection.

Nous nous retrouvons dès lors face à deux aspects incontournables :

- **Premièrement,** être en conformité ne veut pas nécessairement dire qu'on a sécurisé son périmètre. Les objectifs de sécurité provenant de lois, de standards et de réglementations ne peuvent constituer qu'une partie des objectifs globaux de sécurité de l'entreprise. Une bonne gestion de la sécurité va plus que probablement contribuer ou même garantir la mise en conformité, tout en satisfaisant simultanément les besoins de l'entreprise.

- **Deuxièmement,** les efforts en matière de sécurité devraient être alignés et si possible intégrés aux efforts visant à la mise en conformité ou la réduction des risques. Une telle approche évite que les actions et les responsabilités se chevauchent.

3.

— TRADUIRE SON AMBITION DANS UNE POLITIQUE DE SÉCURITÉ DE L'INFORMATION —

La sécurité de l'information est une problématique métier, et non pas uniquement technologique. La motivation d'une entreprise à protéger son information doit naturellement émaner de ses activités et de sa stratégie. Une politique de sécurité s'assure que la vision de l'entreprise en matière de sécurité est traduite dans la pratique. Cette transposition repose généralement sur une politique de haut niveau, de laquelle découlent des directives et des normes, lesquelles sont intégrées dans les procédures opérationnelles de l'organisation.

Une politique de sécurité apporte plusieurs avantages :

- Elle aide les entreprises à rendre visible leur engagement à protéger leurs actifs les plus vitaux ;
- Elle offre un cadre de référence en matière de sécurité de l'information, au travers de l'entreprise, pour tous les métiers et tout le personnel ;
- Elle fait croître la sensibilisation à la sécurité.

Une politique de sécurité pose les fondations de toutes les activités de gestion de la sécurité dans l'entreprise.

4.

— S'ASSURER LE SOUTIEN DE LA DIRECTION —

La fonction de sécurité de l'information doit pouvoir compter sur un engagement fort de l'entreprise envers la cyber-sécurité : ce soutien est essentiel pour pouvoir apporter une réponse rapide et efficace aux menaces sécuritaires actuelles et futures. Par conséquent, le top management doit s'engager, de façon visible, dans la gestion et la supervision de la politique de cyber-sécurité de son entreprise. Il est de son devoir de veiller à ce que les ressources requises – en termes de budget et de personnel – soient allouées à la protection de l'entreprise. Cet engagement se traduit par exemple par la validation formelle de la politique de sécurité par sa direction.

L'équipe dirigeante de l'organisation doit comprendre l'importance que recouvrent les mesures de gestion du risque de cyber-sécurité dans la protection de la réputation, du succès et de la propriété intellectuelle de son entreprise. En effet, protéger son savoir est essentiel pour pouvoir fournir des produits ou des services compétitifs à ses clients.

L'efficacité et l'adéquation des mesures de sécurité de l'information doivent être formellement rapportées :

- De manière régulière, à la plus haute autorité en matière de sécurité au sein de votre entreprise;
- Au moins une fois par an, au conseil de direction et au conseil d'administration.

Ce rapport doit comprendre un certain nombre d'indicateurs et de métriques mesurant la sécurité de l'information, et amener de la visibilité sur la façon dont l'entreprise protège ses actifs. Il est essentiel d'évaluer les progrès et l'efficacité des mesures mises en œuvre en matière de cyber-sécurité, et de permettre que cette information alimente le processus de prise de décision en matière de politique et d'investissements de cyber-sécurité.

5.

— CRÉER UN RÔLE VISIBLE DE SÉCURITÉ DANS L'ENTREPRISE ET RESPONSABILISER CHACUN —

Afin de gérer efficacement la sécurité de l'information, une gouvernance ciblée doit être définie et mise en œuvre. Cette gouvernance doit garantir que les responsabilités en matière de protection de l'information soient assignées aux bonnes personnes, disposant du niveau d'autorité, des formations et des outils nécessaires. De plus, la direction et le soutien à la réalisation de toutes les initiatives en matière de sécurité de l'information doivent être assignés à une fonction spécifique, même si la responsabilité globale en termes de sécurité reste partagée par l'ensemble des acteurs de l'entreprise.

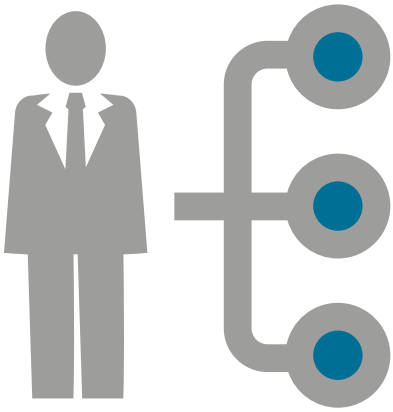
Les plus petites entreprises doivent elles aussi disposer d'une personne qui contrôle régulièrement l'adéquation des mesures de gestion de la cyber-sécurité, et endosse formellement la responsabilité de l'exécution des actions dans ce domaine. Au sein de plus petites structures, ce rôle n'est pas forcément un temps plein, mais il n'est pas moins un rôle essentiel, qui peut d'ailleurs s'avérer vital pour la survie de l'entreprise.

Dans des grandes entreprises, l'allocation des fonctions de cyber-sécurité doit volontairement chercher à impliquer différents représentants de l'organisation au sein de groupes de travail et de comités (éventuellement virtuels). Il est important que chaque participant comprenne parfaitement son rôle et ses responsabilités : la qualité de la documentation et de la communication y jouent donc un rôle essentiel.

L'entreprise doit s'assurer de former son personnel. Elle doit ainsi clairement communiquer sur les responsabilités de chacun, mais également sur les menaces auxquelles l'entreprise est exposée. Une menace importante à laquelle votre personnel doit être formé est l'*ingénierie sociale* : cette technique consiste à manipuler les utilisateurs afin d'obtenir d'eux des informations sensibles ou confidentielles, ou l'exécution d'actions dommageables à l'entreprise (p.ex. un transfert de fonds).

L'organisation doit pouvoir donner les moyens aux quelques personnes clés actives dans la gestion de la cyber-sécurité, de partager des informations utiles avec ses pairs et d'autres intervenants au sein du secteur, tant pour contribuer à l'élaboration de bonnes pratiques en matière de cyber-sécurité, que pour être alertée de nouvelles menaces ou d'attaques potentielles.

Bien que souvent désignés comme le *maillon faible* lorsqu'il s'agit de sécurité de l'information, il est possible de transformer les membres de votre personnel en votre *plus grand atout sécuritaire* : sensibilisez vos équipes à la cyber-sécurité, afin qu'ils prennent conscience des enjeux liés à la sécurité de l'information, et traduisent cette prise de conscience en une série d'actions concrètes au quotidien.



6.

— RESTER SÛR, MÊME EN EXTERNALISANT —

Soutenues par des moyens de communication en continuelle amélioration, les chaînes de valeur de nos entreprises sont devenues fortement intégrées. Les modèles de collaboration avec de tierces parties, tels l'*outsourcing* ou l'*offshoring*, sont ainsi devenus un mode de fonctionnement tout à fait courant.

Cependant toute partie tierce qui ne protègerait pas correctement les informations et les systèmes de ses clients, pourrait être la cause d'incidents ayant le potentiel de lourdement impacter les opérations, la réputation et la valeur de marque d'une entreprise.

Il est dès lors de bonne pratique d'encourager les fournisseurs de services (et en particulier les fournisseurs IT) à respecter au minimum les principes de sécurité appliqués au sein de l'entreprise cliente, mais également d'obtenir l'assurance que les informations et les systèmes d'information dont ils ont la charge sont sécurisés. Une telle assurance peut être obtenue par le biais d'audits des fournisseurs de service ou en exigeant de leur part un rapport formel sur l'état de la sécurité, rédigé par une organisation indépendante. Une attention particulière devrait être portée à la revue et la bonne compréhension du contrat de service, et en particulier des mesures relatives à la disponibilité et la restauration des systèmes, suite à un incident.

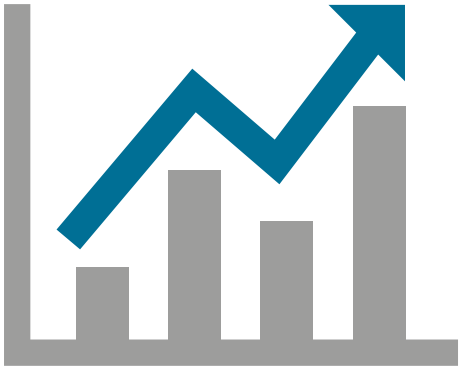
A l'ère des services *cloud* (ou dans le nuage), ce principe est plus que jamais d'application. Les services *cloud* sont l'ensemble des solutions où un fournisseur externe prend en charge le stockage, le traitement ou la gestion des données de l'entreprise au travers d'un réseau tel qu'internet, tout en offrant un haut degré de flexibilité et un contrôle en temps réel des services.

Les fournisseurs de services IT peuvent également offrir des solutions de sécurité. Il est dès lors suggéré d'interroger vos fournisseurs, et notamment vos fournisseurs *cloud*, au sujet des services de sécurité qu'ils proposent au sein ou en complément à leurs solutions. Ces services peuvent par exemple inclure les dispositions de sauvegarde, restauration, ou cryptage de données, qui peuvent s'avérer très intéressants pour une plus petite entreprise.

Il est également recommandé de s'assurer un accès aux traces d'activités (logs) pour l'ensemble des services externalisés. Ces traces sont en effet essentielles quand il s'agit d'analyser et évaluer de menaces en matière de cyber-sécurité.

7.

— S'ASSURER QUE LA SÉCURITÉ SOIT UN MOTEUR POUR L'INNOVATION —



Outre le fait qu'une approche sécuritaire adéquate protège l'entreprise, elle peut également contribuer directement à l'adoption de nouvelles technologies. L'aversion aux risques ne devrait pas empêcher l'introduction de nouvelles technologies : il s'agit simplement de s'assurer que les menaces qui y sont associées soient bien comprises, et qu'elles puissent être mises en rapport avec les bénéfices de cette technologie pour l'entreprise.

L'introduction de solutions et de composants innovants doit s'accompagner de mesures sécuritaires appropriées et ce le plus rapidement possible au court du processus d'adoption, idéalement lors du processus de définition des spécifications fonctionnelles. Le principe de *security by design*, soit une conception intégrant la sécurité, devrait être appliqué afin d'assurer que la sécurité soit prise en compte dès le démarrage de tout développement ou acquisition de nouveaux outils ou d'applications.

Les individus à la source des innovations dans l'entreprise doivent disposer de connaissances en sécurité suffisantes, ou impliquer les experts sécurité, afin d'intégrer lors de la conception de toute nouvelle solution les aspects sécuritaires adéquats.

8.

— SAVOIR SE REMETTRE EN CAUSE —

Les menaces en matière de cyber-sécurité sont en constante évolution. Dans ce contexte, les politiques et procédures de sécurité établies par votre organisation peuvent très vite devenir obsolètes ou tout simplement inefficaces en pratique.

L'exécution d'évaluations régulières du niveau de résistance de l'entreprise aux menaces actuelles en matière de cyber-sécurité et aux vulnérabilités connues, permet de mesurer l'avancement de l'implémentation des mesures de gestion de la cyber-sécurité, et d'évaluer leur adéquation. Ceci peut se faire par des analyses et audits indépendants internes ou externes, tels que des tests de pénétration et scans de vulnérabilités.

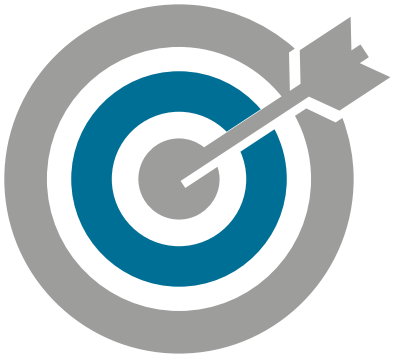
Ces évaluations contribuent également à forger une culture d'entreprise en phase avec les impératifs de cyber-sécurité. Les entreprises devraient permettre aux employés de faire des erreurs et stimuler des discussions ouvertes quant aux incidents de sécurité. C'est ce type de culture qui garantit que les employés ne craignent plus de remonter les incidents quand ceux-ci se produisent.

A côté de ces évaluations, des interactions régulières avec les entreprises issues du même secteur - et plus largement d'autres acteurs du monde des affaires et du milieu judiciaire - peuvent aider l'entreprise à maintenir à jour son niveau de compréhension des menaces présentes et futures en matière de cyber-sécurité.

9.

— RESTER CONCENTRÉ SUR L'ESSENTIEL —

Dans l'économie de la connaissance où nous vivons aujourd'hui, l'information est devenue tout particulièrement précieuse. Bien cerner cet actif, puis s'attacher à l'analyse des vulnérabilités et menaces associées, peut s'avérer une tâche énorme.



Vos efforts doivent donc se concentrer sur la protection des informations les plus précieuses, celles dont un incident lié à leurs confidentialité, intégrité ou disponibilité pourrait sérieusement impacter l'entreprise.

Cela ne signifie pas pour autant qu'il ne faille pas se soucier de la protection des autres informations. Mais ce principe, fondé sur une analyse des risques pour identifier les actifs les plus critiques de l'entreprise, est la manière la plus efficiente et la plus efficace de pratiquer la gestion de la sécurité de l'information. Cette approche rend également clair qu'une élimination totale de tous les risques possibles n'est ni réaliste, ni nécessaire.

10.

— SE PRÉPARER À AFFRONTER DES INCIDENTS —

Un incident de sécurité n'est pas forcément une mauvaise chose. L'important n'est pas l'incident en lui-même mais la manière dont on y répond. Dans notre environnement actuel de menaces et vulnérabilités, la question à se poser n'est pas « Si » mais bien « Quand » on sera victime d'un incident de sécurité… et si on y est préparé.

Votre entreprise doit être préparée, au niveau tant organisationnel que technologique, à faire face à un incident de sécurité de telle manière qu'elle en minimise les impacts sur son activité. Idéalement, des fournisseurs de services spécialisés dans la maîtrise et la remédiation d'incidents de sécurité auront été pro-activement identifiés, pour être prêt le jour où une réaction quasi immédiate se révèle nécessaire.

Un bon plan de réponses aux incidents, qui doit comprendre une stratégie de communication interne et externe, peut faire la différence entre une interruption de votre activité de moins d'un jour, ou une interruption complète longue de plusieurs journées ; entre un fait divers de 10 lignes en page 7 et les grand titres à la Une des journaux.

Il est primordial que les incidents de sécurité soient communiqués de manière appropriée en interne et si nécessaire en externe. De plus, il faut garder à l'esprit que rapporter de tels incidents aux autorités compétentes est une manière de contribuer à l'amélioration du paysage sécuritaire, et que par ailleurs, c'est dans certains cas une obligation.

PRÉVENIR VAUT TOUJOURS MIEUX QUE GUÉRIR

10 ACTIONS À ENTREPRENDRE EN MATIÈRE DE SÉCURITÉ

La rubrique suivante fournit une synthèse des actions clés que toute entreprise devrait envisager d'intégrer à son approche de la sécurité de l'information. Ces actions visent à soutenir l'entreprise dans différentes phases de la gestion de la cyber-sécurité : la *protection* de l'entreprise contre les incidents, la *détection* d'un cas d'incident, la *maîtrise* d'un incident, la *réaction* à un incident, et le *rétablissement* de l'activité à la suite d'un incident.

1.

— SENSIBILISER ET FORMER LES UTILISATEURS À LA SÉCURITÉ —

La sécurité de l'information est un sujet qui touche toute l'entreprise. Les personnes qui créent et manipulent l'information d'une entreprise jouent également un rôle majeur dans la sauvegarde de cette information. Si elles ne respectent pas des principes de précaution élémentaires, elles peuvent devenir source d'incidents de sécurité, voire pire, faciliter fortement la tâche d'attaquants.
Il est essentiel de maintenir, au sein de l'entreprise dans son ensemble, une connaissance des principales menaces et défis en matière de cyber-sécurité. **Les sujets suivants sont cités en guise d'exemple :**

- Comment communiquer en toute sécurité et de manière responsable
- Comment utiliser les médias sociaux de manière judicieuse
- Comment transférer les fichiers numériques de manière sécurisée
- Comment utiliser son mot de passe de façon appropriée
- Comment éviter la perte d'informations importantes
- Comment s'assurer que seules les bonnes personnes puissent accéder à vos données
- Comment se protéger des virus et autres logiciels malveillants (*malware*)
- Qui avertir lorsque vous constatez un incident de sécurité potentiel
- Comment ne pas se faire piéger et divulguer des informations à des tiers malveillants

Cette connaissance permet de s'assurer que tous les membres du personnel ayant accès aux informations et systèmes de l'entreprise, comprennent le rôle qu'ils jouent dans sa protection, et contribuent à cette protection dans leurs tâches quotidiennes. Un environnement de travail où les réflexes de cyber-sécurité sont la norme se met alors en place, faisant de la sécurité une partie intégrante de la culture de l'entreprise. Répéter régulièrement les messages relatifs à la cyber-sécurité est la meilleure façon de progressivement développer les compétences de sécurité souhaitées au sein de vos équipes.

Comme la plupart des membres du personnel utilisent également Internet à des fins privées, les actions de formation ne doivent pas se limiter uniquement à l'utilisation de l'information de l'entreprise. Il est important que votre personnel comprenne aussi comment protéger leur vie et données privées.
Vous trouverez une source générale d'information sur la cyber-sécurité et la sensibilisation des utilisateurs sur www.safeonweb.be, une initiative du CERT.be (l'équipe fédérale d'intervention d'urgence en sécurité informatique) et sur http://www.enisa.europa.eu/media/multimedia/material, une initiative d'ENISA. L'utilisation des informations, vidéos, images et autres matériels disponibles sur ces sites à des fins éducatives au sein de l'entreprise est autorisée.

2.

— MAINTENIR SES SYSTÈMES À JOUR —

Bon nombre de piratages et infections virales informatiques exploitent des failles de sécurité pour lesquelles des solutions et correctifs sont disponibles, souvent même depuis plus d'un an avant l'incident.

Systèmes et logiciels, en ce compris l'équipement réseau, doivent être mis à jour dès que des correctifs et mises à jour logicielles sont publiées. Ces mises à jour et correctifs de sécurité corrigent des vulnérabilités de système dont des pirates informatiques pourraient abuser.

Dès qu'ils sont disponibles à des conditions commerciales acceptables, après les tests nécessaires et dès que possible en général, utilisez les services de mise à jour automatiques, en particulier pour des systèmes de sécurité comme les applications anti-malware (p.ex. anti-virus), les outils de filtrage Web et les systèmes de détection d'intrusion.

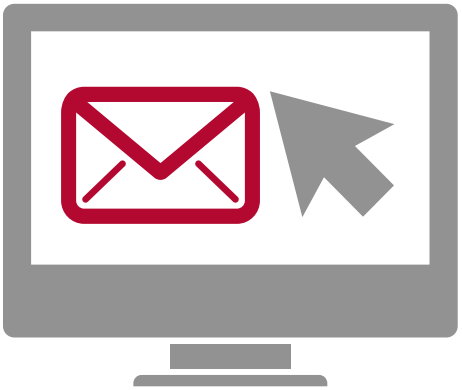
Afin de s'assurer que tous les systèmes fassent l'objet d'une protection adéquate, il est conseillé de maintenir un inventaire de ces systèmes, accompagné de la liste des exigences minimales de sécurité applicable à chacun d'entre eux.

Seules les mises à jour logicielles de sécurité directement fournies par le fournisseur d'origine devraient être acceptées, afin de garantir leur authenticité. Aucune action de mise à jour logicielle ne devrait être réalisée sur base d'un correctif en pièce jointe d'un e-mail, ou sur base d'un lien vers un site inconnu.

3.

— PROTÉGER L'INFORMATION —

Plus que jamais, la stratégie de sécurité de l'information doit se concentrer sur les données plutôt que sur des technologies sécuritaires. La sécurité du périmètre réseau et le contrôle d'accès traditionnel ne sont plus suffisants, en particulier lorsque l'information est stockée dans des environnements hors de votre contrôle, comme internet ou des supports mobiles.



Différentes techniques de cryptage sont disponibles et ont démontré leur efficacité dans des circonstances spécifiques (qu'il s'agisse de stockage ou de transport de données), par exemple :

- Les e-mails envoyés via internet à des partenaires commerciaux, clients et autres, le sont par défaut en texte clair. Les entreprises doivent fournir les moyens à ses utilisateurs de crypter les e-mails lorsque les informations transmises sont sensibles.

- Les équipements portables tels que les ordinateurs portables, clés USB et smartphones peuvent constituer des cibles privilégiées pour des voleurs, ou sont parfois perdus. C'est pourquoi les entreprises doivent s'assurer qu'ils sont soit cryptés par défaut (ordinateurs portables et smartphones), soit cryptés à la discrétion de l'utilisateur (clés USB).

4.

— SÉCURISER LES APPAREILS MOBILES —

Les équipements portables sont une source de défis considérables en matière de gestion et de sécurité, en particulier lorsqu'ils contiennent des informations sensibles et confidentielles, ou lorsqu'ils peuvent se connecter au réseau de l'entreprise :

- Perte de données
- Attaques d'ingénierie sociale
- Logiciel malveillant (*malware*)
- Menaces pour l'intégrité des données
- Abus de ressources
- Attaques basées sur le Web et le réseau
- …

Le concept BYOD (*Bring Your Own Device* – utilisation du matériel privé pour accéder au réseau de l'entreprise) est très séduisant pour beaucoup d'organisations et d'employés, mais comporte l'inconvénient d'accroître le risque d'exposition de l'information sensible de l'entreprise.

Par conséquent, il est nécessaire d'adopter une position claire quant aux appareils qui sont autorisés à accéder au réseau et/ou à l'information de l'entreprise, et adopter une politique et des procédures appropriées en matière de sécurité.

Les utilisateurs doivent protéger l'accès à leurs appareils portables par un mot de passe fort. Les entreprises doivent proposer et / ou imposer aux utilisateurs de configurer l'appareil mobile de façon sûre, le protégeant ainsi des tentatives d'individus malveillants de voler l'information qu'ils contiennent. Le système d'exploitation et les logiciels installés sur ces appareils doivent être tenus à jour, en particulier ceux de sécurité, afin de rester protégés contre les dernières versions des malwares et des virus.

En outre, des procédures de rapport immédiat de tout vol ou perte d'équipement doivent être disponibles ainsi que, si possible, des fonctionnalités de nettoyage à distance permettant de supprimer toutes les informations de l'entreprise présentes sur les équipements perdus ou volés. **Les utilisateurs doivent également rester vigilants vis à vis de leur environnement, tant avant que pendant l'utilisation de leurs équipements portables. Ils doivent également adopter les comportements suivants:**

- Installer des solutions de sécurité des e-mails
- Éviter d'ouvrir des messages inattendus provenant d'expéditeurs inconnus
- Éviter d'ouvrir des liens non identifiés
- Éviter de chatter avec des personnes inconnues

5.

— RESTREINDRE LES ACCÈS AUX AUTORITÉS NÉCESSAIRES —

Un accès ne doit être délivré que s'il s'avère justifié par la fonction professionnelle ou dans le cadre d'une tâche à accomplir. Personne ne devrait avoir accès à tous les systèmes et données.

Les privilèges d'administrateur système (*root, superuser, administrator*) ne doivent être accordés qu'à un nombre limité d'employés dignes de confiance. De nos jours, il existe des options qui permettent aux administrateurs système de faire leur travail sans avoir accès aux données.

Les responsables d'applications et de données devraient régulièrement (au moins une fois par an) revoir et valider les droits d'accès dans leurs domaines respectifs.

En outre, les employés ne devraient pas pouvoir installer un logiciel sur les ordinateurs – fixes ou portables – de l'entreprise sans autorisation préalable. Ils ne devraient pas non plus pouvoir modifier les paramètres de sécurité des applications, du système d'exploitation, ou des logiciels de sécurité, et ne devraient pas pouvoir désinstaller ces logiciels de sécurité. Ces accès sont soumis à un risque significatif d'incidents et devraient par conséquent être considérés comme un privilège et être uniquement accordés aux personnes qui en ont réellement besoin.

6.

— APPLIQUER DES RÈGLES DE SÉCURITÉ POUR LA NAVIGATION SUR INTERNET —

En ce qui concerne l'accès à des services sur internet, d'un point de vue strictement sécuritaire, seuls les services dont les employés ont besoin dans leurs fonctions devraient être accessibles. Néanmoins, nombreuses sont les entreprises qui adoptent des politiques de ressources humaines autorisant une utilisation privée d'internet sur le lieu de travail, tant qu'elle reste raisonnable et en accord avec les valeurs éthiques de l'entreprise. Dans ce cas, le blocage de services internet pour raison de sécurité devrait au minimum couvrir ceux qui comportent le plus haut niveau de risque, à savoir les sites offrant des logiciels piratés ou malveillants, les sites offrant des services de partage de fichiers de poste à poste (*peer to peer*), ou encore les sites dédiés aux activités de piratage informatique ou au contournement de contrôles de sécurité. Un autre risque auquel s'expose l'entreprise est celui de violation du droit d'auteur, qui peut se matérialiser suite au téléchargement et à l'utilisation non autorisée de logiciels ou autre contenu protégé (photographies, documents, musique, vidéo...).

Il existe des solutions qui catégorisent chaque service sur internet et permettent de filtrer le contenu disponible sur base de ces catégories, de manière configurable et flexible (sur base de quota, en fonction du jour et de l'heure, etc). Il est essentiel que les règles de navigation sur internet en vigueur au sein de votre entreprise soient transparentes pour tous les utilisateurs. L'entreprise doit également disposer d'un mécanisme permettant d'ouvrir l'accès aux sites et services bloqués par défaut, mais qui s'avèrent nécessaires pour le travail.
Les risques qu'implique la navigation sur internet ne se limitent pas aux virus et logiciels espions distribués via certains sites malveillants. En effet, l'ouverture à internet rend également l'entreprise plus vulnérable à l'hameçonnage (*phishing*)[3] , et augmente ainsi le risque que des informations privées ou professionnelles soient volées.

Les versions récentes des navigateurs les plus populaires intègrent la possibilité de bloquer une liste de sites Web frauduleux connus. **C'est pourquoi tout équipement utilisé pour accéder à internet devrait disposer d'un tel navigateur. Les utilisateurs devraient être informés des astuces permettant de reconnaître les sites Web malveillants, telles que:**

- Vérifier que le site dispose d'une section de contact avec une adresse, un numéro de téléphone et/ou une adresse e-mail qui peut être validée, ainsi qu'une politique de protection de la vie privée.
- Contrôler la destination réelle d'un hyperlien en passant avec le curseur sur ce lien (sans cliquer) et en regardant (généralement) dans le coin inférieur gauche du navigateur où l'adresse réelle du site Web de destination s'affiche.
- Contrôler que l'adresse Web commence par 'https://' avant d'introduire des informations personnelles ou confidentielles.

[3] http://en.wikipedia.org/wiki/Phishing : action de tenter d'acquérir des informations, comme des noms d'utilisateurs, des mots de passe, et des données de cartes de crédit (et parfois, indirectement, de l'argent) en faisant croire à la victime qu'elle s'adresse à un tiers de confiance dans une communication électronique.

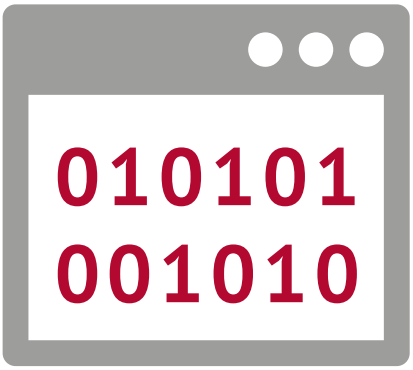
7.

— ADOPTER DES MOTS DE PASSE FORTS, ET LES STOCKER EN SÉCURITÉ —

Les mots de passe sont le principal moyen utilisé pour protéger vos informations. Par conséquent, il est primordial que des mots de passe forts soient utilisés. Pour vous assurer qu'un mot de passe est fort, vous devez mettre en œuvre et imposer un certain nombre de principes:

- Chaque utilisateur doit disposer d'un identifiant unique et personnel, réservé à son usage exclusif. Il ne peut en conséquence pas partager le mot de passe associé à cet identifiant.
- Une longueur de mot de passe et une complexité minimales doivent être imposées afin de s'assurer que ces mots de passe soient suffisamment difficiles à deviner.
- Les utilisateurs doivent être tenus de changer leurs mots de passe périodiquement (tous les 3 mois est une bonne pratique).
- Les utilisateurs doivent utiliser des mots de passe différents pour accéder à des applications différentes.
- Les utilisateurs sont tenus de ne pas mélanger des mots de passe personnels et des mots de passe professionnels.

Pour des accès critiques, tels que l'accès à distance au réseau de l'entreprise, une méthode d'authentification multi-facteurs est à envisager.



En présence d'une authentification multi-facteurs, l'entreprise devra sélectionner les facteurs à utiliser parmi au moins deux des trois principes suivants:

- Quelque chose que je connais (p.ex. mot de passe ou code PIN)
- Quelque chose que j'ai (p.ex. une carte à puce ou un token d'authentification qui génère des mots de passe dynamiques à usage unique)
- Quelque chose que je suis (p.ex. empreinte digitale ou reconnaissance de l'iris)

Le choix des facteurs doit également prendre en compte les contraintes réglementaires applicables, et l'acceptabilité du moyen d'authentification par le personnel.

8.

— SAUVEGARDER SES DONNÉES, ET CONTRÔLER LES SAUVEGARDES —

Un élément tout aussi critique que la protection de la confidentialité et de l'intégrité des données est celui de la sauvegarde de ces dernières. Au cas où l'information est volée, perdue, modifiée ou effacée par erreur, la disponibilité d'une copie de sauvegarde peut se révéler cruciale.

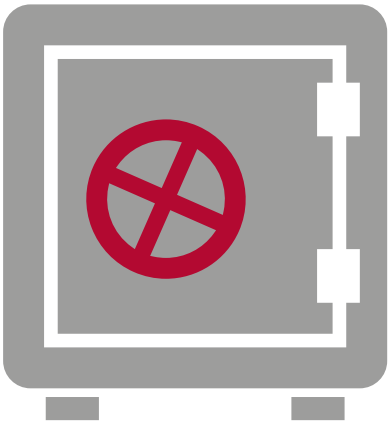
Une politique de sauvegarde doit être mise en place, et préciser :

- quelles données sont sauvegardées , et comment elles le sont ;
- à quelle fréquence les données sont sauvegardées ;
- qui est responsable de la création de sauvegardes ;
- où et comment les sauvegardes sont stockées ;
- qui a accès à ces sauvegardes ;
- quelles procédures suivre pour restaurer des données à partir de sauvegardes.

Lors de la définition de cette politique, assurez-vous que les exigences légales et réglementaires concernant la rétention d'informations soient prises en compte et respectées.

Gardez à l'esprit que les supports physiques de sauvegarde tels que les CD, bandes magnétiques ou disques durs sont eux-mêmes exposés à une série de vulnérabilités (p.ex. accès non autorisé). Dès lors, les copies de sauvegarde doivent bénéficier du même niveau de protection que les données dont elles sont issues, en particulier en ce qui concerne la sécurité physique, étant donné que ces supports peuvent être facilement déplacés.

Un des problèmes les plus fréquemment rencontrés dans la gestion des sauvegardes se situe au niveau de la validation du contenu des copies de sauvegarde. Il arrive trop souvent que lorsqu'une restauration de contenu est nécessaire, on s'aperçoive que la sauvegarde est inutilisable.



Par conséquent, il faut instaurer une discipline garantissant le test régulier de la restauration des sauvegardes afin de s'assurer de leur bon fonctionnement, d'en vérifier l'exhaustivité et de tester la vitesse de récupération des données. Dans l'éventualité où des tiers interviennent dans le stockage de l'information (p.ex. des services de type *Cloud*), ils doivent veiller à ce que des dispositions similaires soient prises pour la sauvegarde de cette information.

9.

— LUTTER À DIFFÉRENTS NIVEAUX CONTRE LES VIRUS ET AUTRES PROGRAMMES MALVEILLANTS —

En raison de la grande variété des systèmes et des besoins des utilisateurs, une protection efficace contre les virus et autres logiciels malveillants requiert l'adoption de plusieurs lignes de défense. Un logiciel antivirus est indispensable, mais il ne doit pas être la seule protection d'une entreprise. Une combinaison de plusieurs techniques pour se protéger contre les virus est nécessaire pour garantir une sécurité adéquate.

L'alliance de l'utilisation d'un filtrage Web, d'une protection antivirus, d'une protection proactive contre les *malwares*, de pare-feux , de politiques solides en matière de sécurité et d'une formation des utilisateurs réduit considérablement le risque d'infection. Envisagez d'utiliser des marques différentes de technologies pour des fonctions similaires (ex. des vendeurs différents pour les solutions logicielles de protection contre les *malwares*). Maintenir le logiciel de protection à jour conjointement avec le système d'exploitation et les applications accroît la sécurité effective des systèmes.

10.

— PRÉVENIR, DÉTECTER ET AGIR —

Les entreprises ne réalisent souvent pas qu'un incident de sécurité est en train de se produire. Il arrive que des systèmes restent infectés et pillés pendant des mois, ou même des années, avant que l'intrusion ne soit détectée… quand elle est effectivement détectée.

Les entreprises doivent investir à la fois dans des systèmes de prévention et des systèmes de détection d'intrusion. L'efficacité de ces outils varie en fonction de la qualité de leur mise en œuvre et de la formation des utilisateurs. Recherchez des tiers expérimentés pour des conseils et du support lorsque ces connaissances n'existent pas au sein de votre entreprise.

Au-delà des aspects technologiques, les professionnels affichant un intérêt pour la cyber-sécurité peuvent profiter de partenariats à différents niveaux : sectoriels, industriels, gouvernemental voire même à un niveau international, avec des initiatives comme le *World Economic Forum's Partnering for Cyber Resilience* (partenariat pour la cyber-résilience du Forum Économique Mondial).

En cas d'incident de sécurité avéré, les entreprises doivent envisager de faire un rapport à l'équipe fédérale d'intervention d'urgence en sécurité informatique (CERT.be), dont l'adresse e-mail est cert@cert.be. Le rapport au CERT permet de déterminer si l'incident est isolé ou pas. Une attaque peut être horizontale (différentes entreprises du même secteur sont ciblées) ou verticale (des sous-traitants de l'entreprise ciblée sont également attaqués), ou peut encore être une menace associée à un logiciel ou un matériel particulier. Le CERT sera capable de fournir certaines informations et certains conseils relatifs à l'incident susceptibles d'aider la victime à définir des contre-mesures efficaces.
Les organisations qui sont victimes de la (cyber) criminalité doivent également introduire une plainte auprès de la police. La police locale n'est pas spécialisée et est plutôt un point de contact pour la criminalité traditionnelle. Pour les cas de cyber-criminalité (piratage, sabotage, espionnage), il est préférable de s'adresser directement à la *Federal Computer Crime Unit* (FCCU), en particulier lorsqu'il s'agit d'une attaque sur une infrastructure informatique critique ou vitale. Il est également possible de contacter indépendamment le bureau du procureur du Roi. Une plainte aidera en outre la justice à se faire une image plus précise de la cyber-menace pour les entreprises en Belgique.

En traitant un incident de sécurité, et en particulier un cas de cyber-criminalité, les responsables (informatiques) devraient dès le départ s'assurer d'une bonne préservation des preuves. Des directives pour l'acquisition par le personnel informatique de données qui peuvent constituer des indices ou preuves dans le cadre d'une investigation d'incident de sécurité[4], ou en cas d'infection par un *malware*[5], sont disponibles en ligne sur le site Web du CERT-EU.

[4] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf
[5] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf

COURT ET SIMPLE

QUESTIONNAIRE D'AUTO-ÉVALUATION

La rubrique suivante présente un questionnaire simple qui peut guider la direction d'une entreprise dans l'examen de ses capacités de résilience à des menaces de cyber-sécurité, en proposant les questions clés à poser aux équipes impliquées. Ce questionnaire a été conçu pour permettre d'identifier les forces et les faiblesses de l'organisation, et mettre en avant les pistes d'amélioration à suivre pour renforcer son niveau de résilience.

Ce questionnaire peut également être utilisé comme une *checklist* par les entreprises qui en sont à leurs débuts en matière de sécurité : les questions et réponses listées peuvent alors permettre de structurer un plan d'implémentation d'un dispositif complet de cyber-sécurité.

Pour chacune des questions qui suivent, il convient de choisir l'option qui reflète le mieux les pratiques actuelles de l'entreprise. Chacune des options s'est vue attribuer un point de couleur, suivant les principes suivants :

C'est la réponse la moins souhaitable ; des améliorations doivent absolument être envisagées.

Quelques améliorations supplémentaires pourraient être apportées, afin de mieux protéger l'entreprise.

Cette réponse correspond à la situation recommandée, afin d'offrir un niveau de résilience suffisant face aux menaces de cyber-sécurité.

En outre, la présence d'*une checklist détaillée au-dessous de chaque question* permet d'identifier et de documenter l'état d'une série de contrôles de sécurité de base au sein de l'entreprise.

Pour chaque question, un lien avec les actions et principes décrits dans les deux précédents chapitres est proposé : ce lien permet aux répondants d'utiliser les actions et principes du Guide comme lignes directrices lors de la définition de plans d'actions.

1. EVALUEZ-VOUS LA SENSIBILITÉ DES INFORMATIONS AU SEIN DE VOTRE ENTREPRISE?

✘ Non, mais nous avons un pare-feu pour nous protéger du vol d'informations.

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

✔ Oui, et nous disposons d'un modèle de classification de l'information et nous savons où nos données sensibles sont stockées et traitées. Les mesures de sécurité que nous mettons en œuvre, le sont en fonction du niveau de sensibilité de l'information concernée.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Vos données sensibles sont-elles identifiées et classifiées ?		
Êtes-vous conscient de vos responsabilités liées aux informations identifiées comme sensibles (lois, réglementations, mesures internes, …) ?		
Les données les plus sensibles sont-elles particulièrement protégées ou cryptées ?		
La gestion des données à caractère personnel est-elle couverte par des procédures spécifiques ?		
Vos employés sont-ils tous capables de différencier des données sensibles de données non sensibles, et de les traiter en fonction ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

2. EVALUEZ-VOUS LES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION ?

✘ Nous n'exécutons pas d'évaluations de risque.

O Nous exécutons des évaluations de risque, mais pas spécifiquement sur des sujets relatifs à la sécurité de l'information.

✔ Nous accomplissons des évaluations de risque sur des sujets relatifs à la sécurité de l'information.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Abordez-vous les vulnérabilités détectées par niveau de risque, du niveau le 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 telles interruptions est-il évalué?		
Disposez-vous d'un plan de continuité de l'activité (business continuity plan) qui est régulièrement testé et mis à jour ?		
Menez-vous régulièrement une évaluation des risques, permettant de réévaluer vos besoins en termes de cyber-sécurité ?		
Identifiez-vous les zones de risque au sein de vos différents processus métier, afin de définir les mesures requises pour contrer la corruption de vos données ou l'utilisation malveillante de cette information ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

3. À QUEL NIVEAU SE PLACE LA RESPONSABILITÉ DE LA SÉCURITÉ DE L'INFORMATION AU SEIN DE VOTRE ORGANISATION ?

✘ Il n'y a pas de gouvernance spécifique à la sécurité de l'information au sein de notre entreprise.

○ Une gouvernance de la sécurité de l'information existe, et est installée au sein du département informatique, étant donné que ce sont ces équipes qui doivent agir pour sécuriser l'information.

✔ Une gouvernance de la sécurité de l'information existe, et est installée au niveau de la direction de l'entreprise, afin de s'assurer que l'ensemble de l'entreprise soit concernée par la gestion de la cyber-sécurité.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les membres du conseil d'administration allouent-ils un budget à la sécurité de l'information ?		
La sécurité de l'information fait-elle partie des pratiques de gestion du risque de la direction ?		
La direction approuve-t-elle la politique de sécurité de l'entreprise, et s'assure-t-elle de sa diffusion au personnel ?		
Les membres du conseil d'administration et la direction de l'entreprise sont-ils régulièrement informés des dernières évolutions des politiques, normes ou procédures de gestion de la sécurité de l'entreprise ?		
Est-ce qu'au moins un membre de la direction a la charge de la protection des données et de la protection de la vie privée ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

L'ACTION SUIVANTE PEUT ÊTRE PRISE :

4. DISPOSEZ-VOUS D'UNE ÉQUIPE OU D'UNE FONCTION DÉDIÉE À LA GESTION DE LA SÉCURITÉ DE L'INFORMATION ?

✘ Nous n'avons pas d'équipe dédiée à la sécurité de l'information, et n'avons pas spécifiquement alloué de rôles ou responsabilités en la matière.

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

✔ Nous avons une équipe ou une fonction spécifiquement en charge de la gestion de la sécurité de l'information.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Est-ce qu'un spécialiste ou une équipe sécurité coordonne la gestion des compétences en matière de sécurité, et assiste la direction dans la prise de décision sur les sujets de sécurité?		
Est-ce que le responsable ou l'équipe sécurité a la responsabilité de revoir et mettre à jour la politique de sécurité en fonction des évolutions de l'entreprise, ou des incidents de sécurité rencontrés ?		
Est-ce que le responsable ou l'équipe sécurité dispose de suffisamment de visibilité et de soutien managérial pour intervenir dans toute initiative liée à l'information ?		
Différents managers sont-ils responsables des différents types de données ?		
Faites-vous régulièrement évaluer par un organe indépendant (interne ou externe) si votre politique de sécurité est réaliste et efficace et l'action de l'équipe de sécurité performante ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

L'ACTION SUIVANTE PEUT ÊTRE PRISE :

5. COMMENT GÉREZ-VOUS LES RISQUES DE SÉCURITÉ LIÉS AUX FOURNISSEURS QUI ACCÈDENT À VOS DONNÉES SENSIBLES ?

✘ Nous avons une relation fondée sur la confiance mutuelle avec nos fournisseurs.

● Pour certains contrats, nous incluons des clauses relatives à la sécurité de l'information.

✔ Nous avons des processus en place pour valider l'accès des fournisseurs à nos données, et avons établi des directives de sécurité spécifiques qui sont communiquées et signées par nos fournisseurs.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les fournisseurs et autres parties externes sont-ils identifiés par un badge d'identification, lequel comprend une photo récente ?		
Avez-vous une politique de contrôle des antécédents de vos sous-traitants et fournisseurs ?		
Les accès à vos bâtiments et systèmes sont-ils automatiquement désactivés lorsqu'un sous-traitant ou un fournisseur termine sa mission ?		
En cas de perte ou vol d'information, vos fournisseurs savent-ils comment et à qui immédiatement rapporter cet incident au sein de votre entreprise ?		
Votre entreprise s'assure-t-elle que les fournisseurs maintiennent leurs logiciels et applications à jour (et notamment, installent les mises à jour de sécurité) ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

L'ACTION SUIVANTE PEUT ÊTRE PRISE :

6. FAITES-VOUS ÉVALUER RÉGULIÈREMENT LA SÉCURITÉ INFORMATIQUE ET DE RÉSEAU ?

✘ Nous n'effectuons pas d'audit ou de test d'intrusion pour évaluer notre sécurité informatique et de réseau.

○ Nous n'avons pas d'approche systématique pour commanditer des audits de sécurité et/ou des tests de pénétration mais en exécutons occasionnellement.

✔ Des audits de sécurité réguliers et / ou des tests d'intrusion font systématiquement partie de notre approche pour évaluer notre sécurité informatique et de réseau.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Faites-vous des tests réguliers, et documentez-vous les menaces ainsi identifiées ?		
Disposez-vous de procédures visant à évaluer les menaces humaines, telles que la malhonnêteté, l'ingénierie sociale et l'abus de confiance ?		
Votre entreprise exige-t-elle des rapports d'audit de sécurité auprès de ses fournisseurs de services informatiques ?		
L'utilité de chaque type de données stockées est-elle également évaluée pendant les audits de sécurité ?		
Faites-vous auditer vos procédures et processus de gestion de la sécurité, pour vous assurer de leur conformité avec les autres politiques et normes établies au sein de l'entreprise ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

7. LORSQU'ELLE INTRODUIT DE NOUVELLES TECHNOLOGIES, VOTRE ENTREPRISE ÉVALUE-T-ELLE LES RISQUES POTENTIELS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ?

✘ L'évaluation des risques en termes sécurité de l'information ne fait pas partie du processus de mise en œuvre de nouvelles technologies.

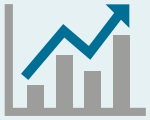
● La gestion de la sécurité de l'information est parfois considérée lors de la mise en œuvre de nouvelles technologies, mais cela n'est pas systématique.

✔ La gestion de la sécurité de l'information est incluse dans le processus de mise en œuvre de nouvelles technologies.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Lorsque vous envisagez de mettre en œuvre de nouvelles technologies, évaluez-vous l'impact potentiel sur la politique de sécurité de l'information de votre organisation ?		
Disposez-vous de mesures de protection qui réduisent les risques éventuellement liés à la mise en œuvre de nouvelles technologies ?		
Les processus de mise en œuvre de nouvelles technologies sont-ils documentés ?		
Avez-vous noué des partenariats avec d'autres acteurs, dans une optique de collaboration et d'échange d'informations utiles relatives à la sécurité lors de l'implémentation de nouvelles technologies ?		
La politique de sécurité de votre entreprise est-elle souvent considérée comme un frein à l'innovation technologique ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

8. LA SÉCURITÉ DE L'INFORMATION A-T-ELLE UNE PLACE DANS VOTRE ORGANISATION?

✘ Nous avons confiance en nos employés et nous ne considérons pas qu'un accompagnement plus important en matière de sécurité apporte de la valeur ajoutée à l'entreprise.

O Seul notre personnel informatique reçoit une formation spécifique pour sécuriser notre environnement informatique.

✔ Des sessions de sensibilisation à la sécurité sont régulièrement organisées, à l'attention de tous les employés.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Adaptez-vous le contenu de certaines sessions de sensibilisation au métier et à l'activité des participants (et aux menaces qui sont liées à cette activité, spécifiquement) ?		
Formez-vous vos équipes à être attentives aux violations des principes et mesures de sécurité ?		
Votre entreprise dispose-t-elle d'instructions claires à l'attention des utilisateurs, expliquant comment rapporter des faiblesses ou des menaces sécuritaires liées à vos systèmes ou à vos activités ?		
Votre personnel connaît-il les bonnes pratiques à suivre en termes d'utilisation des données de cartes de crédit et de gestion d'informations à caractère personnel ?		
Les autres utilisateurs de vos systèmes (p.ex. fournisseurs ou clients) sont-ils également formés en matière de sécurité et informés des évolutions de vos politiques et procédures de sécurité ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

L'ACTION SUIVANTE PEUT ÊTRE PRISE :

9. COMMENT UTILISEZ-VOUS LES MOTS DE PASSE AU SEIN DE L'ENTREPRISE ?

✘ Nous partageons les mots de passe avec d'autres collègues et / ou il n'existe pas de politique définissant les règles liées à l'usage sûr des mots de passe ou leur renouvellement régulier.

○ Tous les employés, y compris la direction, possèdent des mots de passe uniques, mais des règles relatives à la complexité de leur composition ne sont pas imposées. Le changement des mots de passe est possible, mais pas obligatoire.

✔ Tous les employés, y compris la direction, disposent d'un mot de passe personnel qui doit satisfaire à des exigences précises en matière de complexité et doit être changé régulièrement.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise a-t-elle établi et implémenté une politique en matière de mot de passe ?		
Avez-vous les moyens de garantir que tous les mots de passe ont été changés au moins une fois et sont régulièrement modifiés, correspondent à vos exigences de complexité, et ne sont pas stockés dans des fichiers facilement accessibles, et ce aussi pour les appareils mobiles ?		
Vous sentez-vous bien protégé contre un accès physique non autorisé à vos systèmes ?		
Vos utilisateurs, tant internes qu'externes, ont-ils conscience de leur responsabilité en termes de protection des équipements laissés sans surveillance (p.ex. conscients de l'importance de mettre fin à sa session avant de quitter son poste) ?		
Les employés ont-ils été formés à l'identification de tentatives d'ingénierie sociale, et aux façons de réagir à une telle menace ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

10. DISPOSEZ-VOUS D'UNE POLITIQUE RELATIVE À LA BONNE UTILISATION D'INTERNET ET DES MÉDIAS SOCIAUX ?

✘ Non, nous ne disposons pas d'une politique relative à la bonne utilisation d'internet et des médias sociaux.

O Oui, une telle politique placée à un endroit accessible par tous les employés a été publiée, mais elle n'a pas été signée par chaque membre du personnel.

✔ Oui, une telle politique existe et a été signée par chaque membre du personnel, ou fait partie de son contrat de travail.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Existe-t-il des directives à l'attention de tout membre du personnel, définissant les règles relatives aux communications effectuées au nom de l'entreprise (y compris vers la presse ou sur les médias sociaux) ?		
Existe-t-il un processus disciplinaire pour les employés qui violent les directives de communication de l'entreprise ?		
Est-ce que l'équipe ou le responsable communication de l'entreprise passe régulièrement internet en revue afin d'évaluer la 'réputation en ligne' de l'entreprise, et les éventuels risques qui la menace ?		
Votre entreprise a-t-elle évalué comment sa responsabilité serait engagée, en cas d'utilisation de ses systèmes par des utilisateurs internes ou des pirates afin de perpétrer des actes illégaux ?		
Votre entreprise a-t-elle pris des mesures pour empêcher un employé ou tout autre utilisateur interne d'attaquer d'autres sites ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

11. EST-CE QUE VOTRE ENTREPRISE MESURE, RAPPORTE ET ASSURE LE SUIVI DES SUJETS RELATIFS À LA SÉCURITÉ ?

✘ Nous ne contrôlons pas, nous ne rapportons pas et nous ne suivons pas ni l'efficacité ni l'adéquation des mesures de sécurité que nous avons mises en œuvre.

○ Nous avons des outils et méthodes pour mesurer, rapporter et suivre tant l'efficacité que l'adéquation de certaines de nos mesures de sécurité, mais pas toutes.

✔ Notre entreprise a mis en œuvre les outils et méthodes nécessaires pour mesurer l'efficacité et l'adéquation de toute mesure de sécurité mise en œuvre, faire le rapport de ces évaluations, et faire le suivi des éventuels points d'amélioration.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les traces systèmes (traces d'audit et logs) relatives aux incidents sont-elles toujours conservées, et des actions sont-elles prises pour empêcher que l'incident ne se reproduise ?		
Votre entreprise contrôle-t-elle son degré de conformité aux exigences légales et réglementaires (p.ex. la protection des données à caractère personnel) ?		
Disposez-vous d'outils permettant aux managers d'évaluer le niveau global de sécurité de leurs activités, et leur offrant les moyens de répondre plus rapidement à d'éventuels risques de sécurité ?		
Votre entreprise dispose-t-elle d'une feuille de route relative à la sécurité de l'information, qui définisse notamment les objectifs à atteindre et les indicateurs de progrès à suivre ?		
Les rapports de contrôle et d'incidents sont-ils partagés avec les autorités compétentes, et avec d'autres groupes d'intérêts tels qu'une fédération sectorielle ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

L'ACTION SUIVANTE PEUT ÊTRE PRISE :

12. COMMENT MAINTENEZ-VOUS VOS SYSTÈMES À JOUR ?

✘ Nous nous basons sur la gestion automatique des correctifs telle que proposée par le fournisseur pour la plupart de nos solutions.

O Nous installons les correctifs de sécurité systématiquement, à intervalles réguliers (p.ex. sur base mensuelle).

✔ Nous disposons d'un processus de gestion des vulnérabilités par lequel nous nous tenons constamment à jour sur d'éventuelles nouvelles vulnérabilités (par ex. via un abonnement à un service d'alertes signalant toute nouvelle vulnérabilité), et nous appliquons les correctifs rapidement, en fonction du niveau de risque lié à la vulnérabilité qu'ils solutionnent.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Des scans de vulnérabilités sont-ils planifiés et régulièrement exécutés au sein de l'entreprise ?		
Les applications sont-elles revues et testées, après tout changement au niveau des systèmes d'exploitation ?		
Les utilisateurs peuvent-ils contrôler eux-mêmes si les applications sont bien à jour (aucun patch de sécurité manquant) ?		
Les utilisateurs sont-ils conscients qu'au niveau de leurs appareils mobiles, ils doivent également maintenir à jour le système d'exploitation et les applications qui y sont installées (y compris les applications de sécurité) ?		
Avez-vous formé vos utilisateurs à reconnaître d'éventuels faux messages d'avertissement systèmes (p.ex. demandant l'autorisation de mettre un logiciel à jour, ou émanant d'un faux antivirus) et à systématiquement avertir vos équipes de sécurité si un tel évènement suspect s'est produit ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

13. LES DROITS D'ACCÈS SONT-ILS RÉGULIÈREMENT REVUS ?

✘ Les droits d'accès des utilisateurs aux applications et systèmes de l'entreprise, ne sont pas retirés ou revus de façon structurée et systématique.

O Les droits d'accès des utilisateurs aux applications et systèmes de l'entreprise sont uniquement retirés lorsqu'un employé quitte l'entreprise ; il n'y a pas de processus de revue régulière des accès existants.

✔ Une politique de contrôle d'accès est en place et inclut des revues régulières des droits d'accès assignés aux utilisateurs pour toutes les applications et systèmes pertinents de l'entreprise.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
L'accès électronique et physique aux systèmes d'information est-il restreint, sur base de politiques et procédures de gestion des accès ?		
Votre entreprise s'appuie-t-elle sur une politique de protection de la vie privée indiquant l'information qu'elle recueille (par exemple concernant vos clients : les adresses physiques, les adresses électroniques, l'historique de navigation, etc.), et la façon dont cette information est exploitée ?		
Vos politiques et procédures de gestion des accès précisent-elles quelles méthodes doivent être utilisées pour contrôler l'accès physique à des zones sécurisées (p.ex. installation de portes, systèmes de contrôle d'accès, surveillance vidéo, …) ?		
Les droits d'accès aux systèmes et aux bâtiments de votre entreprise sont-ils automatiquement désactivés lorsqu'un membre du personnel quitte votre entreprise ?		
Les données sensibles sont-elles classifiées (p.ex. confidentiel, sensible, usage interne,...) et les utilisateurs ayant droit d'y accéder inventoriés ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

14. VOS EMPLOYÉS PEUVENT-ILS UTILISER LEURS APPAREILS PERSONNELS (SMARTPHONES, TABLETTES, ...) POUR STOCKER OU TRANSFÉRER DES INFORMATIONS DE L'ENTREPRISE ?

✘ Oui, nos employés peuvent stocker ou transférer des informations de l'entreprise sur des appareils personnels, sans que nous exigions la mise en œuvre de mesures de sécurité supplémentaires.

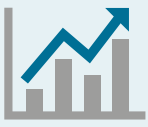
● Il existe une politique qui interdit l'utilisation d'appareils personnels pour stocker ou transférer des informations de l'entreprise, mais techniquement, nos employés peuvent les utiliser et ne sont pas forcés à mettre en œuvre des mesures de sécurité supplémentaires.

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

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise dispose-t-elle d'une politique de Bring Your Own Device, autorisant le personnel à utiliser ses appareils mobiles personnels moyennant une série de conditions ?		
Les appareils mobiles sont-ils protégés contre l'accès par des utilisateurs non autorisés ?		
Les appareils mobiles et les connexions sont-ils/elles identifié(e)s de manière permanente sur le réseau ?		
Les données des appareils mobiles sont-elles cryptées, afin de protéger leur confidentialité et leur intégrité ?		
Votre direction est-elle consciente que si chaque employé est responsable de son appareil personnel, c'est l'entreprise qui est responsable des données professionnelles qu'il pourrait contenir ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

15. VOTRE ENTREPRISE A-T-ELLE PRIS DES MESURES CONTRE LA PERTE D'INFORMATIONS?

✘ Nous ne disposons pas de processus de gestion des sauvegardes ou de mécanismes garantissant la disponibilité de nos données.

○ Nous disposons de processus de gestion des sauvegardes et de mécanismes garantissant la disponibilité de nos données. Cependant, aucun test de ces processus (restauration des données sauvegardées, …) n'a été réalisé.

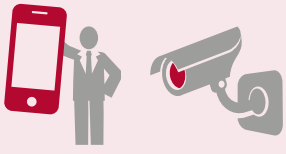
✔ Nous disposons d'un processus de gestion des sauvegardes et de mécanismes garantissant la disponibilité de nos données, lesquels incluent des tests de restauration / de résilience. Nous stockons des copies de nos sauvegardes sur un autre site sécurisé ou nous utilisons d'autres solutions de 'haute disponibilité des données'.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise compte-t-elle suffisamment d'employés capables de sauvegarder ou archiver vos données selon des méthodes qui permettent de rapidement les restaurer ?		
Vos équipements sont-ils protégés des coupures de courant par le biais de systèmes d'alimentation électrique permanente (utilisation de différentes lignes électriques, onduleurs[6], générateurs électriques, etc.) ?		
Les supports de sauvegarde (tape, disques, etc.) sont-ils régulièrement testés, afin de vous assurer que vos données peuvent être restaurées dans les limites de temps définies?		
Votre entreprise dispose-t-elle de procédures garantissant que la perte ou le vol d'équipements portables sont immédiatement notifiés ?		
Vos employés sont-ils formés afin de savoir comment réagir en cas de suppression accidentelle de données, ou comment récupérer ces données en cas de désastre ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



[6] Aussi connu sous le nom de UPS, ou 'Uninterruptible Power Supply'

16. VOTRE ENTREPRISE EST-ELLE PRÉPARÉE À GÉRER UN INCIDENT LIÉ À LA SÉCURITÉ DE L'INFORMATION ?

✘ Nous ne craignons pas d'incident. Et si un incident survient, nos employés sont suffisamment compétents pour y faire face.

○ Nous avons des procédures de gestion des incidents, inadaptées toutefois au traitement des incidents en matière de sécurité de l'information.

✔ Nous avons un processus dédié au traitement des incidents liés à la sécurité de l'information, ainsi que les dispositifs d'escalation et de communication nécessaires. Nous nous efforçons de traiter les incidents de la manière la plus performante et efficace possible, et d'en tirer les leçons qui nous permettront de mieux nous protéger à l'avenir.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre processus prend-il en compte différents types d'incidents - du déni de service (denial of service) à la violation de confidentialité, etc. - ainsi que les moyens d'y faire face ?		
Votre entreprise dispose-t-elle d'un plan de communication intégré au processus de gestion des incidents ?		
Avez-vous identifié les autorités auxquelles notifier un incident, et comment procéder à cette notification ?		
Disposez-vous de points de contacts (et de leurs coordonnées) identifiés pour chaque type d'incident ?		
Vous reposez-vous sur un représentant du service de communication interne de votre entreprise, pour les contacts avec les employés et leurs familles ?		

LE PRINCIPE SUIVANT S'APPLIQUE :

LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

ÉTUDES DE CAS

ÉTUDES DE CAS

Nous avons rassemblé quelques études de cas qui décrivent chacune comment une entreprise a appliqué (ou n'a pas appliqué) certains des principes et des actions décrits dans ce Guide. Ces cas démontrent ainsi que les principes et les actions présentés s'appliquent à toute organisation, indépendamment de sa taille ou de sa complexité.

1.

— UNE GRANDE ENTREPRISE NATIONALE (SECTEUR INDUSTRIEL) ACTIVE À L'INTERNATIONAL —

L'entreprise dont il est question ici se spécialise dans le façonnage et le meulage de composants pour machines-outils. Elle s'appuie d'ailleurs fortement sur des ordinateurs spécialisés, intégrés à son environnement de production. Outre ces outils de production, on ne retrouve dans l'atelier que quelques ordinateurs de bureau, directement connectés au réseau interne de l'entreprise, et essentiellement utilisés pour l'exécution de tâches administratives. Voici quelques temps, le personnel du service de maintenance a également choisi d'utiliser ces ordinateurs de bureau pour transférer, d'une manière plus efficace, les mises à jour logicielles depuis le réseau de l'entreprise vers les ordinateurs de la chaîne de production.

Pendant les pauses, le personnel de maintenance utilise ces mêmes ordinateurs de bureau pour naviguer sur internet, jouer à des jeux ou se connecter sur les réseaux sociaux. Arrive alors ce qui devait arriver : à son insu, l'un des utilisateurs installe un logiciel malveillant sur l'une de ces machines. Une fois installé, le logiciel espion se met au travail, envoyant des informations relatives aux activités de cet ordinateur vers un hôte externe malveillant. Ce même logiciel espion télécharge de nouveaux *malwares*, et notamment un logiciel déclenché en fonction de la date et l'heure, et empêchant les machines infectées de démarrer sans qu'un mot de passe spécifique ne soit inséré.
Ignorant tout de l'infection, le personnel du service de maintenance poursuit ses activités quotidiennes, et met régulièrement à jour les ordinateurs de la chaîne de production, répandant ainsi le *malware* dans tout l'environnement opérationnel de l'organisation. En l'espace d'une semaine, trois des ordinateurs de la chaîne de production ne démarrent plus, tout comme d'ailleurs l'ensemble des ordinateurs de bureau de l'atelier de production, tous infectés.

Un consultant spécialisé en sécurité technique est alors engagé pour examiner les ordinateurs. Il y découvre une panoplie de *malware*, et notamment des logiciels de rançonnage (*ransomware*) tournant "en coulisse". Il note qu'un *keylogger*, un dispositif enregistrant tout ce que tape un utilisateur au clavier de l'ordinateur (nom d'utilisateur, mot de passe, adresse IP, …), est intégré au logiciel espion. Ce dispositif est identifié comme la méthode utilisée par les cyber-criminels pour parvenir à accéder aux systèmes de l'entreprise, et d'y installer la 'bombe à retardement' qui a verrouillé, un à un, les ordinateurs infectés.

Un logiciel de sécurité, comprenant un logiciel antivirus et anti-espion, était bien installé sur ces ordinateurs. Toutefois, les mises à jour automatiques du logiciel n'étaient pas activées, ne garantissant donc pas que le logiciel de sécurité puisse reconnaître les derniers virus et *malware* en circulation. Par ailleurs, aucun scan régulier et automatique des machines n'est programmé, ne permettant pas la vérification régulière de la santé du système. Les autres ordinateurs de l'entreprise étant eux correctement configurés, l'infection ne s'est pas répandue au-delà de l'atelier de production.
Sur les ordinateurs infectés, un message apparaît, qui exige que l'entreprise effectue un virement sur un compte bancaire donné, afin de recevoir une clé numérique spéciale qui débloquerait les ordinateurs. Tant que dure l'infection, la capacité de production de l'entreprise est considérablement réduite, et le montant de la rançon, relativement limité, est nettement inférieur au coût de l'installation de nouveaux systèmes de production : l'équipe de direction décide donc rapidement de virer le montant demandé. Une fois débloqué, chaque ordinateur est entièrement nettoyé par le consultant spécialisé, et réinstallé pour un usage opérationnel. L'entreprise décide en outre de ne pas entamer de poursuites judiciaires, ni de signaler l'incident à la police.

Bien qu'ayant choisi de ne pas porter plainte, la direction de l'entreprise décidera de former les membres du personnel actifs dans les ateliers de production, eux aussi, à ses politiques internes en matière de sécurité de l'information. Par ailleurs, elle informera ses fournisseurs, partenaires et concurrents de l'incident dont elle a été victime, jetant ainsi les bases d'une relation de confiance dans le cadre de laquelle pourront s'échanger toutes informations relatives à de tels incidents de sécurité.

2.

— UN DÉTAILLANT DE TAILLE MOYENNE ACTIF DANS LE COMMERCE EN LIGNE —

Cette entreprise est un grand détaillant international, exerçant ses activités en Belgique et à l'étranger, et comptant plus de 6 millions de clients en Europe. Sur sa plateforme de vente en ligne, chaque client peut créer son propre profil, contenant des données personnelles. L'entreprise stocke également des données relatives aux préférences des utilisateurs, l'historique de leurs activités et leurs centres d'intérêts. Afin de protéger ces données sensibles des pirates et autres *malwares*, l'entreprise a décidé de protéger tous ses sites Web.

Le site Web opérationnel traite des milliers de transactions chaque jour, et fait appel à différentes technologies de différents fournisseurs pour gérer ces fonctionnalités. Cette entreprise a donc mis en place un système de détection de fraude, capable de détecter de (potentielles) transactions frauduleuses. Par ailleurs, elle exécute très régulièrement des tests sur les différents systèmes soutenant la plateforme de commerce en ligne, sur base de catalogues régulièrement mis à jour des vulnérabilités connues.

Lorsque des risques sont détectés, ils sont automatiquement et instantanément remontés vers une équipe spécialisée rassemblant des développeurs, des professionnels de la sécurité et des représentants des différents métiers de l'entreprise. Ceux-ci se réunissent régulièrement pour discuter de ces risques potentiels, et contrôler que les vulnérabilités détectées ont été résolues par la prise de mesures appropriées.

Cette entreprise a décidé d'automatiser certaines parties de son processus de gestion de la sécurité, en raison de la nature de ses activités en ligne et des risques que sa présence en ligne induit. Elle a également décidé de systématiquement faire revoir la sécurité de tout nouveau développement de ses programmes et sites Web, par le biais d'une revue de code réalisée par une entreprise spécialisée et des tests de la sécurité de ses plateformes, même après que les fonctionnalités ont été publiées.

L'infrastructure supportant ces plateformes est régulièrement adaptée afin de refléter les nouvelles exigences et besoins en matière de sécurité - ils évoluent constamment - et de rester un acteur technologiquement agile sur son marché. Ses systèmes requièrent l'installation de correctifs (*patches*) presque chaque jour, afin de corriger rapidement toute faille de sécurité nouvellement détectée dans l'un des produits ou l'une des technologiques qu'elle utilise. Elle autorise également des scans externes de son infrastructure, puisqu'ils lui permettent de dresser un rapport sur les vulnérabilités potentielles et existantes.

Les tentatives d'accès aux données personnelles et autres informations sensibles que gère cette entreprise, sont permanentes, et émanent tant de pirates que d'utilisateurs autorisés. De par la nature de ses activités, l'entreprise accepte qu'un jour viendra où elle sera, elle aussi, piratée : son équipe de direction s'y est préparée, et elle dispose de procédures pour gérer de tels incidents, notamment pour assurer une communication structurée, efficace et adéquate.

3.

— UNE PME COMPTABLE —

Cette petite entreprise familiale de comptabilité compte parmi ses clients de longue date, une série de PME mais aussi de très grandes entreprises. En 2012, l'entreprise est frappée par une série de *malwares*, combinant des virus et des chevaux de Troie. L'un de ces virus corrompt les fichiers et les rend inutilisables : il cible tout particulièrement les documents Microsoft Word et les feuilles de calcul Microsoft Excel, ce qui, pour une entreprise fortement dépendante de la suite Microsoft Office pour ses activités, se révèle extrêmement dommageable. Le virus désactive également les fonctions de sécurité du logiciel antivirus installé, permettant ainsi des infections ultérieures d'autres virus.

On découvrira par la suite que ce virus s'est répandu par le biais d'un logiciel téléchargeable gratuitement, appelé *Defense Center*, et qui se présente comme un outil de sécurité gratuit permettant de protéger l'utilisateur contre les menaces de sécurité.

Ce logiciel provenait d'un site Web et a été installé par un utilisateur sur son ordinateur. Dès son installation terminée, ce *malware* commence à attaquer l'ordinateur de l'utilisateur : il active un cheval de Troie, un morceau de code qui transmet aux auteurs du logiciel pirate toutes les données nécessaires pour se connecter à l'ordinateur infecté.

À chaque fois qu'un utilisateur ouvre un document Microsoft Office, le *malware* infecte le document et continue à répandre le virus aux différents contacts e-mail de l'utilisateur. Les destinataires d'un e-mail ont l'habitude d'ouvrir les pièces jointes d'une personne en qui ils ont confiance. Seules les entreprises disposant de systèmes antivirus récemment mis à jour auront pu détecter le virus intégré dans les pièces jointes. Ce sont ces destinataires qui contacteront rapidement l'entreprise infectée afin de lui signaler l'incident.

Le *malware* s'est répandu si rapidement via le réseau interne de l'entreprise, vers d'autres ordinateurs, que tous ont rapidement et sans exception été infectés. Ce logiciel malveillant détruit progressivement tous les fichiers .xls (feuilles de calcul Excel) et .doc (documents Word) stockés sur les disques durs en les remplaçant par le texte "DATAError". Une perte des données d'une telle ampleur aurait pu entraîner non seulement une interruption totale de l'activité de la société, mais également sa faillite pure et simple. Heureusement, l'entreprise possède un système de sauvegarde efficace : à la fin de chaque semaine, toutes les données sont sauvegardées directement depuis chaque ordinateur de chaque employé, et copiées sur un nouveau DVD qui est daté et stocké en toute sécurité en dehors du site. Alors que les données des ordinateurs infectés ont été perdues, elles pourront être récupérées à partir des DVD de sauvegarde. Si l'entreprise parviendra à récupérer la plupart des fichiers grâce à ces sauvegardes, elle aura toutefois perdu trois jours de travail complets, c'est-à-dire les fichiers créés ou modifiés entre la date de la dernière sauvegarde et la date de l'infection.

Les différents e-mails infectés auront pu contourner la sécurité du réseau, car ils étaient téléchargés par des utilisateurs légitimes, derrière le pare-feu. Cet incident aura souligné le besoin d'une formation adéquate du personnel quant à l'utilisation d'internet, et une révision des procédures de sauvegarde visant à en augmenter la fréquence, et assurer des tests réguliers de restauration de ces sauvegardes pour s'assurer qu'elles puissent toujours être exploitées.

4.

— UNE START-UP BELGE —

Cette jeune start-up propose un agrégateur de demande et d'offre énergétique entièrement automatisé, offrant aux opérateurs de réseaux d'énergie une solution permettant de faire face aux pics de demande qui peuvent potentiellement déstabiliser le réseau. Elle se repose pour cela sur des acteurs industriels, gros consommateurs d'énergie capables de limiter brièvement leur consommation sans que cela n'ait d'impact négatif sur leur production. Le service proposé par cette jeune start-up se repose sur sa propre plateforme technologique, permettant une automatisation complète de l'intégralité du service.

Le besoin de sécurité

Le besoin de sécurité de l'information au niveau de cette jeune entreprise est motivé par deux éléments clés :

1. **Le couplage de leur plateforme à des systèmes critiques pour leurs clients.** La plateforme technologique de cette entreprise est directement connectée à des centres de contrôle d'opérateurs de réseau d'énergie, ainsi qu'à des systèmes de gestion automatisée d'installations industrielles. Deux éléments qui font partie des cibles les plus critiques et les plus exposées aux cyber-attaques. Tout incident de sécurité endommagerait gravement la réputation et les perspectives commerciales de la jeune entreprise.
2. **Le secret de fabrication.** En tant que jeune entreprise technologique, la technologie qu'elle a développée et dont elle détient les droits et le secret, est le tout premier de ses différentiateurs. À ce titre, cette information doit tout particulièrement être protégée de ses concurrents et de toute autre partie externe.

Sensibilisation de la direction et du personnel

- Le conseil d'administration a souligné à plusieurs reprises le besoin de mettre l'accent sur la sécurité, en encourageant l'entreprise à définir des politiques claires et à protéger les secrets de fabrication et la propriété intellectuelle.
- Des principes et procédures en matière de gestion d'informations confidentielles ont été définis et communiqués à l'ensemble de l'entreprise.
- L'équipe Recherche & Développement de l'entreprise est soumise à des directives spécifiques en termes d'authentification forte et de cryptage des mots de passe, et met un accent particulier sur la sécurité dans chacune des étapes du processus de développement.

Plan d'action

Les points suivants constituent la synthèse du programme défini par cette entreprise, afin d'implémenter un cadre complet de gestion de la sécurité de l'information.

Mesures en cours d'implémentation :

1. Mesures techniques :
   a. La plateforme de l'entreprise est hébergée dans des centres de données à la pointe du progrès, également en termes de sécurité.
   b. Les clients les plus critiques sont connectés à la plateforme par le biais d'un réseau dédié, tandis que les autres clients sont connectés par le biais des connexions hautement sécurisées (tunnels IPsec) où des règles strictes en matière de pare-feu sont appliquées.
   c. Le contrôle d'accès se repose sur une authentification à deux facteurs, combinant un token matériel (fournit une clé d'authentification unique, valide quelques secondes) et des mots de passe forts, gérés de manière stricte.
2. Mesures organisationnelles :
   a. Le niveau de confidentialité de chaque document est défini, et systématiquement renseigné sur le document lui-même.
   b. Les accès à ces informations sont restreints aux personnes qui en ont le besoin spécifique.
3. Mesures procédurales :
   a. Différents niveaux d'autorisation ont été définis, par groupe d'utilisateurs, sur la plateforme.
   b. Une jeune entreprise de petite taille ne peut se permettre de dédier du personnel à la sécurité exclusivement. Pour cette raison, un audit externe a été demandé en 2013 afin d'effectuer un examen structurel du niveau de sécurité de la start-up, et une évaluation complète des risques en matière de sécurité de l'information.

Actions prévues à moyen terme :

1. Un spécialiste en sécurité énergétique réalisera une analyse détaillée des manquements et des risques de sécurité ;
2. Cette jeune entreprise vise à obtenir le certificat ISO 27001/2 en 2014, adoptant ainsi une approche proactive pour devenir une entreprise plus sûre ;
3. La start-up investira donc du temps et des efforts sur une année complète pour préparer cette certification, en se concentrant sur la mise en œuvre de procédures de gestion de la sécurité, la sensibilisation continue de ses équipes et le développement d'un modèle de contrôle permanent de la sécurité.

LA CYBER-SÉCURITÉ EN BELGIQUE – LISTE DE CONTACTS

LA CYBER-SÉCURITÉ EN BELGIQUE – LISTE DE CONTACTS

Notez qu'une liste de ces contacts et leurs coordonnées est constamment tenue à jour sur le site **www.b-ccentre.be**. Cette liste de contacts est divisée entre les organes et organisations publiques d'une part, et quelques organisations sans but lucratif d'autre part. La description du rôle en matière de sécurité de l'information de chaque organisation sélectionnée, dans chaque catégorie, provient généralement de l'organisation elle-même. Si par ailleurs, vous souhaitez de plus amples renseignements sur les services fournis en matière de sécurité de l'information par des firmes commerciales, nous vous invitons à consulter leur site web, comme par exemple **www.ey.com/BE/** ou **www.microsoft.com/belux/**.

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISMES PUBLICS ET ORGANISATIONS		
BANQUE NATIONALE DE BELGIQUE	**www.nbb.be** **Banque Nationale de Belgique** Avenue de Berlaymont 14 1000 Bruxelles Belgique +32 2 221 21 11 info@nbb.be Fonctions opérationnelles spécifiques dans le domaine de la surveillance prudentielle tf@nbb.be	La Banque Nationale de Belgique a publié des directives détaillées s'adressant à toutes les institutions financières en matière de sécurité de l'information.
B-CCENTRE	**www.b-ccentre.be** **Belgian Cybercrime Centre of Excellence for Training, Research and Education** Sint-Michielsstraat 6 3000 Leuven Belgique +32 16 32 07 82 contact@b-ccentre.be	Le B-CCENTRE est un projet placé sous la coordination de la KU Leuven, qui mutualise les efforts déployés par des chercheurs universitaires, des entreprises commerciales et des organisations publiques dans le cadre de la lutte contre la cybercriminalité. Le B-CCENTRE offre une plateforme destinée à échanger informations et connaissances en Belgique et est le partenaire belge d'un réseau européen de centres où des informations sur la lutte et la protection contre la cybercriminalité peuvent être intégrées et diffusées à tous les intéressés. Le Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) est une organisation regroupant un large nombre d'acteurs contre la cyber-criminalité en Belgique. Initiative coordonnée par l'Interdisciplinary Centre of Law et l'ICT à la KU Leuven, le B-CCENTRE est la principale plateforme de collaboration et de coordination en matière de cyber-criminalité en Belgique. Il combine une grande expertise en termes de groupes de recherche universitaires, acteurs du secteur et organisations publiques en un vaste réseau de connaissances. Ses principales activités englobent la recherche fondamentale interdisciplinaire, l'organisation de formations et la facilitation d'une prise de conscience au travers de l'enseignement.

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISMES PUBLICS ET ORGANISATIONS		
CERT.be	**www.cert.be** **Federal Cyber Emergency Team** Avenue Louise 231 1050 Bruxelles Belgique +32 2 790 33 33 cert@cert.be	Le CERT.be est le premier point de contact belge lorsqu'il s'agit de traiter des menaces et vulnérabilités de la cyber-sécurité affectant les intérêts belges. Les professionnels des technologies de l'information et de communication (ICT) peuvent s'adresser gratuitement au CERT.be et en toute confidentialité pour faire rapport de cyber-incidents (données et infrastructures réseau piratées, hameçonnage (*phishing*), cyberattaques, etc.). Le CERT.be donne également des conseils aux citoyens et aux entreprises sur la façon d'utiliser internet en toute sécurité. Plus d'informations sont disponibles sur www.cert.be (pour les entreprises) et www.safeonweb.be (pour les citoyens).
COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE	**www.privacycommission.be** **Autorité belge pour la protection des données** Rue de la Presse 35 1000 Bruxelles Belgique +32 2 274 48 78 commission@privacycommission.be	L'Autorité belge pour la protection des données a pour mission essentielle de veiller à ce que la vie privée soit respectée lorsque des données personnelles sont traitées. Il s'agit d'un organisme fédéral belge. L'Autorité belge pour la protection des données a publié des directives claires sur comment gérer correctement les incidents relatifs à la vie privée dans le cyber-monde.
CRID	**www.unamur.be/droit/crids** **Centre de Recherche Information, Droit et Société** Rue de Bruxelles 61 5000 Namur Belgique +32 81 72 40 00	Le CRIDS regroupe une dizaine d'académiques et plus de 40 chercheurs, qui, ensemble, tissent un champ de compétences très vaste, de l'histoire de l'informatique, à la protection de la vie privée, des nouveaux modes de gouvernance à la production de biens culturels communs, du droit des communications électroniques au récit de soi sur internet, de la protection des consommateurs numériques ou des patients « électroniques » au corps technologique. Il s'est impliqué dans de nombreux projets de recherche en matière de cyber-sécurité et a publié plusieurs livres blancs sur le sujet.
ENISA	**www.enisa.europa.eu** **http://cybersecuritymonth.eu/** **European Network & Information Security Agency** Science and Technology Park of Crete Vassilika Vouton, 700 13 Heraklion Grèce +30 28 14 40 9710 info@enisa.europa.eu	L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est la réponse de l'Union Européenne face aux problèmes de cyber-sécurité de l'Union. À ce titre, elle est en première ligne en ce qui concerne la sécurité de l'information en Europe, et il s'agit également d'un centre d'expertise. L'objectif consiste à faire du site Web de l'ENISA le hub européen pour l'échange d'informations, de meilleures pratiques et de connaissances dans le domaine de la Sécurité de l'Information.

LISTE DE CONTACTS

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISMES PUBLICS ET ORGANISATIONS		
FCCU	**www.polfed-fedpol.be/crim/crim_fccu_nl.php** **Federal Computer Crime Unit** Rue du Noyer 211 1000 Bruxelles Belgique +32 2 743 74 74	La Federal Computer Crime Unit (FCCU) belge est responsable de la lutte contre la cyber-criminalité et les infractions au niveau des technologies de l'information et de la communication, avec pour but de protéger tous les citoyens dans le cyber-monde contre toutes les formes de criminalité "traditionnelle" et "nouvelle". Cette mission inclut également : la lutte contre d'autres phénomènes criminels bénéficiant d'un soutien d'investigation spécialisé au niveau de l'environnement des technologies de l'information (IT). La fraude dans les services de télécommunications ainsi que la fraude au niveau des cartes de paiement relèvent également de ses compétences.
FEDICT	**www.fedict.belgium.be** **Service Public Fédéral Technologie de l'Information et de la Communication** Rue Marie-Thérèse 1 1000 Bruxelles Belgique +32 2 212 96 00 info@fedict.belgium.be	Le Fedict, le Service Public Fédéral Technologie de l'Information et de la Communication, a lancé diverses campagnes de conscientisation de la sécurité sur internet et conseille de nombreuses agences gouvernementales belges concernant la sécurité de l'information.
IBPT-BIPT	**www.ibpt.be** **Institut belge des services postaux et télécommunications** Ellipse Building - Bâtiment C Boulevard du Roi Albert II, 35 1030 Bruxelles Belgique netsec@bipt.be	L'Institut belge des services postaux et des télécommunications (IBPT) supervise tant le secteur postal que le secteur des télécommunications, aujourd'hui appelées communications électroniques. L'IBPT exécute des tâches de réglementation économique, organisation technique et mise en conformité avec les cadres de contrôle. Le BIPT est impliqué dans la sécurité des réseaux publics et des services de communications électroniques accessibles publiquement.
ICRI	**www.law.kuleuven.be/icri** **Centre interdisciplinaire pour le droit et les technologies de l'information** Sint-Michielsstraat 6 3000 Leuven Belgique +32 16 32 07 90 adminicri@law.kuleuven.be	Le Centre interdisciplinaire pour le droit et les technologies de l'information (ICRI) est un centre de recherche sis à la Faculté de Droit de l'Université de Leuven. Il a été impliqué dans de nombreux projets de recherche en matière de sécurité de l'information et a publié plusieurs livres blancs sur le sujet. L'ICRI coordonne les activités du B-CCENTRE.
SÛRETÉ DE L'ÉTAT	**justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/onafhankelijke_diensten_en_commissies/veiligheid_van_de_staat/** +32 2 205 62 11 info@vsse.be	La Sécurité de l'État, le service de renseignement civil et sécurité de Belgique, a parmi ses fonctions la protection des valeurs fondamentales et des intérêts de l'État. La Sécurité de l'État aide les entreprises belges à se protéger contre les cyber-attaques.

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISATIONS PRIVÉES		
AGORIA	**www.agoria.be** **Agoria** Diamant Building Avenue A. Reyers 80 1030 Bruxelles Belgique +32 2 706 78 00 Ferdinand.CASIER@agoria.be	Agoria, la Fédération belge de l'industrie technologique, soutient ses 1.700 entreprises membres dans leur lutte contre la cyber-criminalité par le biais d'ateliers et d'événements réguliers. L'information fournie vise essentiellement la direction d'entreprises qui souhaitent intégrer des aspects de cyber-sécurité dans leur stratégie commerciale.
BELTUG	**www.beltug.be** **Belgian Telecom User Group (Association d'utilisateurs)** Knaptandstraat 123 9100 Sint Niklaas Belgique +32 3 778 17 83 Info@beltug.be	BELTUG dispose d'un groupe d'intérêt spécial sur la sécurité où ses membres se réunissent et discutent de tous les sujets liés à la sécurité des technologies de l'information (IT). BELTUG a organisé beaucoup de tables rondes et publié plusieurs livres blancs sur la sécurité de l'information.
FEB	**www.vbo-feb.be** **Fédération des Entreprises de Belgique** Rue Ravenstein 4 1000 Bruxelles Belgique +32 2 515 08 11 info@vbo-feb.be	La Fédération des Entreprises de Belgique (FEB) représente plus de 50.000 entreprises, soit 80% de l'emploi dans le secteur privé. La FEB est un partenaire privilégié de plusieurs organismes publics dans un certain nombre de programmes d'action visant à protéger l'économie nationale. Elle s'est associée à ICC Belgium pour prendre l'initiative d'éditer un guide de cyber-sécurité s'adressant à toutes les entreprises belges.
FEBELFIN	**www.febelfin.be** **FEBELFIN** Rue d'Arlon 82 1040 Bruxelles Belgique +32 (0)2 507 68 11 info@febelfin.be	Febelfin, la Fédération belge du secteur financier, assiste ses 268 membres dans la lutte contre la cybercriminalité par le biais d'un partage d'informations et d'une coopération avec tous les intervenants impliqués. Febelfin tient à jour un site web spécial, www.safeinternetbanking.be, et a lancé plusieurs campagnes de sensibilisation en matière de sécurité des opérations bancaires sur internet avec des vidéos « choc ».
ICC BELGIUM	**www.iccbelgium.be** **Comité belge de l'International Chamber of Commerce** Rue des Sols 8 1000 Bruxelles Belgique +32 (0)2 515 08 44 info@iccwbo.be	L'International Chamber of Commerce (ICC) est la plus grande organisation professionnelle au monde. Sa commission ICC mondiale sur l'économie numérique s'interroge sur la cyber-criminalité et le développement éventuel de directives ICC axées sur des questions juridictionnelles auxquelles sont confrontées les entreprises mondiales. D'autre part, via sa division dédiée à la lutte contre la criminalité (Services pour la prévention des délits commerciaux (CCS)) installée au Royaume Uni, des organes de décision et d'autres initiatives, l'ICC combat tous les types de criminalité touchant le commerce, y compris la cyber-criminalité.

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISATIONS PRIVÉES		
ISACA	**www.isaca.be** **ISACA Belgium** Rue Royale 109-111 b.5 1000 Bruxelles Belgique +32 2 219 24 82 president@isaca.be	ISACA est une association internationale de connaissance à but non lucratif rassemblant plus de 110.000 membres individuels dans 160 pays et recherchant une valeur et des sujets fiables concernant l'information et la technologie, notamment l'information et la sécurité de l'information. ISACA fait avancer et valide des compétences et connaissances par le biais des titres de *Certified Information Security Manager* (CISM) (gestionnaire en sécurité de l'information) et *Certified in Risk and Information Systems Control* (CRISC) (agréé en contrôle des systèmes d'information et du risque). ISACA a créé COBIT pour la sécurité de l'information, un cadre professionnel qui aide les entreprises dans tous les secteurs et quel que soit l'endroit où elles se trouvent à maîtriser et gérer la sécurité de leur information. ISACA dispose d'une vaste gamme de livres blancs sur la sécurité de l'information, des sondages et des programmes d'audit.
ISPA	**www.ispa.be** **ISPA** Rue Montoyer 39 b 3 1000 Bruxelles Belgique +32 2 503 22 65 Info@ispa.be	ISPA Belgium est l'association de fournisseurs d'accès à internet actifs en Belgique. En regroupant non seulement les fournisseurs d'accès et de services, mais également les fournisseurs d'hébergement et de transit, ISPA assure que le potentiel d'internet soit pleinement atteint tant du point de vue des consommateurs que des professionnels. ISPA organise des ateliers et événements sur le thème de la cyber-sécurité, et est impliquée dans de multiples projets qui contribuent à un usage plus sûr de l'internet en Belgique.

NOM	DONNÉES DE CONTACT	RÔLE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION
ORGANISATIONS PRIVÉES		
L-SEC	**www.lsec.be** **Leaders in Security** Kasteelpark 10 3001 Heverlee Belgique +32 16 32 85 41 Info@lsec.be	LSEC est une association européenne à but non lucratif située en Belgique et active dans la sensibilisation en matière de sécurité de l'information et l'enseignement depuis plus de 10 ans. L'association regroupe des experts émanant de la branche de la sécurité des TIC, des chercheurs en sécurité des TIC et des utilisateurs finaux pour collaborer activement à des projets visant à soutenir l'amélioration globale de la cyber-sécurité en Europe. Des activités de leadership intellectuel organisées par LSEC sur une base mensuelle informent les chefs d'entreprises, responsables de la sécurité et experts en sécurité sur les défis du moment, les meilleures pratiques et les innovations en matière de cyber-sécurité et sécurité de l'information. LSEC est un partenaire actif des programmes EC FP7 et Horizon 2020 et soutient la stratégie numérique pour l'Europe. LSEC assiste les gouvernements des États membres par des contributions actives dans l'établissement de politiques et le partage d'expertise. LSEC exerce des activités en Belgique, aux Pays-Bas et au Royaume-Uni et travaille avec des partenaires dans d'autres États membres européens. LSEC dirige botvrij.be et fournit une plateforme pour des centres ISAC du secteur. www.lsec.be est le portail de l'expertise et des experts en sécurité de l'information en Belgique.

LES RÉFÉRENTIELS LES PLUS COURANTS DE SÉCURITÉ DE L'INFORMATION ET DE CYBER-SÉCURITÉ

Afin d'aborder la sécurité de l'information, nous vous recommandons de consulter une ou plusieurs des bonnes pratiques suivantes, normes et cadres, reconnus dans le monde entier :

NOM	ORGANISATION	SITE WEB
ISO 22301:2012	**ISO**	http://www.iso.org/iso/home.html
ISO 27XXX series	**ISO**	http://www.iso.org/iso/home.html
COBIT5 pour la sécurité de l'information	**ISACA**	www.isaca.org/cobit
SP800 series	**NIST**	http://csrc.nist.gov/publications/PubsSPs.html
Norme de bonne pratique pour la sécurité de l'information	**ISF**	https://www.securityforum.org/tools/sogp/
CIIP et NCSS	**ENISA**	http://www.enisa.europa.eu/activities/Resilience-and-CIIP
Techniques de formation à la sécurité de l'information	**SANS**	http://www.sans.org/reading-room/
BSIMM	**BSIMM**	http://www.bsimm.com
GAISP	**GAISP**	http://all.net/books/standards/GAISP-v30.pdf
Directives de bonne pratique	**BCI**	http://www.thebci.org/index.php/resources/the-good-practice-guidelines
ISAE 3402 et SSAE 16	**AICPA**	http://isae3402.com/
DMBOK	**DAMA**	http://www.dama.org
SABSA TOGAF	**Groupe ouvert**	http://www.opengroup.org/togaf/
OCTAVE	**CERT**	http://www.cert.org/octave/
EBIOS	**ANSSI**	http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/
PAS 555:2013	**British Standards Institute**	http://www.itgovernance.co.uk/shop/p-1356-pas-555-2013-cyber-security-risk-governance-and-management.aspx
Information Technology Security Evaluation Criteria / Manual	**Bundesamt für Sicherheit in der Informationstechnik**	https://www.bsi.bund.de/EN/Topics/topics_node.html

BIBLIOGRAPHIE

Allen & Overy. (2012). *EU and U.S. propose new cybersecurity strategies.* Londres, Royaume-Uni.
Extrait de
http://www.allenovery.com/publications/en-gb/Pages/EU-and-U-S--propose-new-cybersecurity-strategies.aspx

Bergsma, K. (2011). *Information Security Governance.*
Extrait de
https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Governance

Bescherm je bedrijf.
Extrait de
http://www.beschermjebedrijf.nl

CERT-EU. (2012). Incident Response – Data Acquisition Guidelines for Investigation Purposes version 1.3.
Extrait de
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_004_v1_3.pdf

CERT-EU. (2011). Security White Paper 2011-003 - Guidelines for handling common malware infections on Windows based workstations.
Extrait de
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_003_v2.pdf

CESG. (2012). *10 Steps to Information security.* Gloucestershire, Royaumi-Uni.
Extrait de
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Cyber Security Strategy.be.(2012). Belgique.
Extrait de
http://www.b-ccentre.be

Department for Business, Innovation & Skills. (2012). Cyber Risk Management: A Board Level Responsibility. Londres, Royaume-Uni.
Extrait de
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf

EYGM Limited. (2012). *Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey.*
Extrait de
http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

EYGM Limited. (2013). *Under cyber attack: EY's 2013 Global Information Security Survey.*
Extrait de
http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

Federal Communications Commission, Information security Planning Guide, 2012

Federal Communications Commission. (2012). *Information security Planning Guide*. Washington, DC:
Extrait de
http://www.fcc.gov/cyber/cyberplanner.pdf

Information Security Governance Guide.
Extrait de
http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide

ISACA (2013). *Transforming Cybersecurity: Using COBIT® 5*. USA.
Extrait de
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx

Ministerie van Veiligheid en Justitie. (2011). *De Nationale Cyber Security Strategie (NCSS)*. La Haye, Pays-Bas.
Extrait de
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf

Nationaal Cyber Security Centrum. (2013). *Cybersecuritybeeld Nederland*. La Haye, Pays-Bas
Extrait de
https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-3/1/NCSC+CSBN+3+3+juli+2013.pdf

Open Web Application Security Project (OWASP).
Extrait de
https://www.owasp.org

Safe on Web.
Extrait de
http://www.safeonweb.be.

SANS, Information Security Management, ISO 17799 Audit Check List 1.1, Août 2003

World Economic Forum. (2012). *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines*. Genève, Suisse.
Extrait de
http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

REMERCIEMENTS

COMITÉ DE RÉDACTION :

B-CCENTRE
Belgian Cybercrime Centre of Excellence for Training, Research and Education,
ICRI KU Leuven - iMinds
Mennens, A.
Smeulders, C.

EY Belgium Advisory
Deprez, A.
Dewulf, K.
Wulgaert, T.

FEB - Fédération des Entreprises de Belgique
Dammekens, A.
Darville, C.

ICC Belgique - Comité belge de la Chambre de Commerce Internationale
Bodard, K.
Deré, J.
Maes, M.
Thomaes, R.

ISACA Belgium
Vael, M.

L-SEC
Seldeslachts, U.

Microsoft Belgium
Dekyvere, K.
Schroder, B.

SWIFT
Cross, R.

ADAPTATION EN FRANCAIS :

Defrenne, Vincent – NVISO
Dubois, Olivier - Paradigmo
Gilbert, François-Xavier
Godart, Didier - Dgozone
Hanot, Etienne
Marechal, Dominique
Manet, Pierre
Rapaille, Maxime - STIB-MIVB

COMITÉ DIRECTEUR :

CERT.BE
ELECTRABEL
ENISA
FCCU
FEBELFIN
Guldentops, E.
IBPT
IJE
ISPA
Sécurité de l'État
SPF Économie
UMICORE

NOTES

NOTES

graphic design & production:
www.in-depth.be

publisher:
ICC Belgium
Stuiversstraat 8 rue des Sols
1000 Brussel
België
+32 (0)2 515 08 44
info@iccwbo.be
www.iccbelgium.be

GUIDE BELGE DE LA CYBER-SÉCURITÉ
PROTÉGEZ VOTRE INFORMATION

Le présent guide et les documents qui l'accompagnent
ont été élaborés conjointement par

ICC Belgium, FEB, EY, Microsoft, L-SEC,
B-CCENTRE et ISACA Belgium.

Avec le soutien financier du programme de Prévention et de Lutte contre la Criminalité de l'Union Européenne
Commission Européenne - Direction générale des Affaires intérieures