economie
SPF Economie, P.M.E., Classes moyennes et Energie

# Etes-vous une entreprise 1.0 ou 2.0 ?

# Questionnaire de maturité

Pour vous aider à déterminer le niveau de maturité de votre entreprise en matière de cybersécurité, voici un questionnaire d'auto-évaluation divisé en deux volets :

**Volet A. Questions organisationnelles (10 questions)**

**Volet B. Questions techniques (10 questions)**

Pour chacune des questions, choisissez la réponse qui vous paraît le mieux refléter la réalité de votre entreprise. Chaque réponse se voit attribuer des points :

Incertain (je ne sais pas) : Zéro point

Non : 1 point

Oui mais la mise en œuvre laisse à désirer : 2 points

Oui et la mise en œuvre est effective : 3 points

Le total des points est évalué à la fin du présent questionnaire.

Pour vous aider à mieux intégrer la cybersécurité au sein de votre entreprise, chacune des questions renvoie vers les principes et actions pertinents qui relèvent du Manuel « Cybersécurité, votre entreprise est-elle prête ? ».

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

## Volet A : Questions organisationnelles

### 1. Votre entreprise dispose-t-elle d'une équipe ou d'un point de contact dédié à la gestion de la sécurité de l'information ?

- (0) Incertain
- (1) Non
- (2) Oui mais au sein de l'entreprise, rares sont ceux qui savent qui/comment les contacter
- (3) Oui et au sein de l'entreprise tout le monde sait vers qui se tourner

Pour aller plus loin :

**Entreprise 1.0**

Principe 4. Montrez que vous prenez vos responsabilités

**Entreprise 2.0**

Action 1. Top management impliqué

### 2. Votre entreprise traite probablement des données à caractère personnel mais dispose-t-elle d'un Data Protection Officer (DPO ou « délégué à la protection des données ») ?

- (0) Incertain
- (1) Non
- (2) Oui mais vous ne savez pas de qui il s'agit
- (3) Oui et vous savez comment le contacter

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Principe 4. Prévoyez les dispositions relatives en matière de protection de la vie privée

Action 2. Elaborez une politique de sécurité et un code de conduite

### 3. Votre entreprise a-t-elle effectué une analyse des risques ou une analyse d'impact relative à la protection des données dans les trois derniers mois ?

- (0) Incertain
- (1) Non
- (2) Oui mais vous ne connaissez pas les résultats
- (3) Oui et vous connaissez les mesures correctrices qui depuis ont été mises en œuvre

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Etape 1. Analyse de risques ou « Connaissez-vous vous-même » !

### 4. Votre entreprise dispose-t-elle d'une politique en matière de sécurité de l'information pour les internes (internet, médias sociaux, appareils mobiles...)?

- (0) Incertain
- (1) Non
- (2) Oui mais cette politique n'est pas connue par l'ensemble du personnel
- (3) Oui et cette politique fait l'objet d'une formation/sensibilisation à la cybersécurité pour les employés

Pour aller plus loin :

**Entreprise 1.0**

Principe 5. Mettez votre vision en œuvre

**Entreprise 2.0**

Principe 2. Sensibilisez votre personnel à la sécurité de l'information

Principe 8. Pensez à sécuriser les appareils mobiles

Action 2. Elaborez une politique de sécurité et un code de conduite

Action 11. Sécurisez les accès à distance

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

## 5. Votre entreprise dispose-t-elle d'une politique de sécurité ou de lignes directrices concernant les externes (p.ex. fournisseurs) pouvant accéder à certaines informations (potentiellement) sensibles ?

- 0) Incertain
- (1) Non
- (2) Oui mais il n'est pas toujours facile de faire la différence.
- (3) Oui et les contrats avec les fournisseurs ont des clauses spécifiques, les externes sont clairement identifiés comme tels (badges distincts, accès distincts, etc.) et l'information ne circule qu'en fonction de la politique de classification de l'entreprise.

Pour aller plus loin :

**Entreprise 1.0**

Principe 5. Mettez votre vision en œuvre

**Entreprise 2.0**

Principe 10. Prévoir les relations avec les tiers

Principe 3. Identifiez les informations dont dispose l'entreprise et classifiez-les !

## 6. Votre entreprise donne-t-elle des lignes directrices à ses employés concernant le traitement et la « classification » des informations de nature délicate?

- (0) Incertain
- (1) Non
- (2) Oui mais ces consignes sont si compliquées que personne ne les applique
- (3) Oui et ces consignes sont comprises et appliquées

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Principe 3. Identifiez les informations dont dispose l'entreprise et classifiez-les !

## 7. Votre entreprise dispose-t-elle d'un plan de continuité (BCP) ou d'un plan de rétablissement après une catastrophe (DRP) ou un plan de gestion des incidents ?

- (0) Incertain
- (1) Non
- (2) Oui mais personne ne les connait et/ou ces procédures n'ont jamais été testées
- (3) Oui, le personnel connait ces procédures et des tests réguliers (au moins une fois par an) sont organisés

Pour aller plus loin :

**Entreprise 1.0**

Principe 3. Préparez-vous à réagir

Action 6. Préparez-vous à faire face à des incidents

**Entreprise 2.0**

Principe 7. Concevez un « Incident Management Plan » réaliste

Action 12. Disposez d'un plan de continuité (BCP) et d'un plan de gestion des incidents

## 8. Votre entreprise donne-t-elle des directives à ses employés sur la façon de travailler de manière sécurisée lorsqu'ils sont à l'extérieur de leur environnement habituel de travail (réunions externes, télétravail...)?

- (0) Incertain
- (1) Non
- (2) Oui mais il n'y a pas de VPN
- (3) Oui et les accès sont protégés par un réseau virtuel privé (VPN)

Pour aller plus loin :

**Entreprise 1.0**

Action 4. Surveillez votre environnement informatique

**Entreprise 2.0**

Principe 1. Adoptez une défense multicouche

Action 11. Sécurisez les accès à distance

## 9. Votre entreprise impose-t-elle une politique prévoyant le choix d'un mot de passe fort, la sensibilisation à la protection des mots de passe et le changement régulier de ceux-ci ?

- (0) Incertain
- (1) Non
- (2) Oui mais des mots de passe « forts » sont difficiles à mémoriser. Des post-it trainent partout, des mots de passe sont échangés entre collègues, les mêmes mots de passe sont réutilisés sans cesse…
- (3) Oui et chacun sait comment former un mot de passe fort, où le stocker sans danger et comment échanger des informations entre collègues sans échanger des mots de passe personnels.

Pour aller plus loin :

**Entreprise 1.0**

Action 4. Surveillez votre environnement informatique

**Entreprise 2.0**

Action 8. Gérer les accès à vos ordinateurs et à vos réseaux (authentification multi-factorielle)

## 10. Lors de l'introduction de nouveaux projets, votre entreprise évalue-t-elle l'impact en matière de sécurité de l'information et de protection de la vie privée (security/privacy by design and by default) ?

- (0) Incertain
- (1) Non
- (2) Oui, en principe mais dans les faits…C'est une autre histoire.
- (3) Oui, chaque chef de projet sait qu'il doit inclure ce point dans son agenda et qu'aucun nouveau projet IT ne peut sortir sans avoir pris en considération la sécurité et la protection des données.

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Principe 4. Prévoyez les dispositions en matière de protection de la vie privée

Action 3. Sensibilisez vos travailleurs aux risques cyber

## Volet B Questions techniques

### 11. Votre entreprise organise-t-elle régulièrement des sauvegardes (back-up) de tous ses serveurs ?

- (0) Incertain
- (1) Non
- (2) Oui mais ces sauvegardes ne sont jamais testées et/ou se trouvent juste à côté des serveurs principaux
- (3) Oui et ces sauvegardes sont régulièrement testées (qualité des procédures et qualité des contenus). Ces sauvegardes se trouvent de préférence sur un site autre que le site principal

Pour aller plus loin :

**Entreprise 1.0**

Principe 3. Préparez-vous à réagir

Principe 5. Mettez en œuvre votre vision

Action 1. Sauvegardez vos informations et validez les processus de récupération

**Entreprise 2.0**

Principe 1. Adoptez une défense multicouche

Principe 7. Concevez un « Incident Management Plan » réaliste

Action 12. Disposez d'un plan de continuité (BCP) et d'un plan de gestion des incidents

### 12. Votre entreprise maintient-elle régulièrement ses systèmes (OS) et applications à jour ?

- (0) Incertain
- (1) Non
- (2) Oui mais pas de manière automatique. Chaque membre du personnel doit lui-même mettre à jour son OS et ses applications. Il est difficile de savoir si tout le monde l'a correctement fait

- (3) Oui. L'OS est mis à jour automatiquement et les applications sont revues et testées après tout changement au niveau des systèmes d'exploitation. Des sauvegardes de sécurité (point de restauration) sont organisées juste avant

Pour aller plus loin :

**Entreprise 1.0**

Action 2. Mettez à jour vos systèmes informatiques

**Entreprise 2.0**

Action 5. Mettez à jour tous les programmes

## 13. Votre entreprise a-t-elle installé un pare-feu entre les ordinateurs de votre entreprise et internet?

- (0) Incertain
- (1) Non
- (2) Oui mais personne ne sait vraiment comment cela fonctionne
- (3) Oui et du personnel (interne ou externe) qualifié analyse régulièrement les rapports et prend les mesures nécessaires le cas échéant

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Principe 1. Adoptez une défense multicouche

Action 8. Gérez les accès à vos ordinateurs et à vos réseaux

## 14. Votre entreprise dispose-t-elle d'un outil de filtrage ou de blocage des spams ou de phishing ?

- (0) Incertain
- (1) Non

- (2) Oui mais personne ne sait comment repérer un spam/un phishing ni comment réagir face à ce type d'e- mail
- (3) Oui et le personnel est formé pour reconnaître et réagir correctement face à un spam/un phishing

Pour aller plus loin :

**Entreprise 1.0**

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

**Entreprise 2.0**

Principe 1. Adoptez une défense multicouche

Principe 2. Sensibilisez votre personnel à la protection de l'information

Action 3. Sensibilisez vos travailleurs aux risques cyber

## 15. Votre entreprise utilise-t-elle une protection contre les programmes malveillants (malwares) ?

- (0) Incertain
- (1) Non
- (2) Oui, mais pas sur tous les ordinateurs de l'entreprise
- (3) Oui, sur tous les ordinateurs et ces outils sont régulièrement mis à jour

Pour aller plus loin :

**Entreprise 1.0**

Action 2. Mettez à jour vos systèmes informatiques

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

**Entreprise 2.0**

Principe 1. Adoptez une défense multicouche

Action 5. Mettez à jour tous les programmes

Action 6. Installez une protection anti-virus

Action 9. Sécurisez les postes de travail et les appareils mobiles

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

## 16. Votre entreprise utilise-t-elle un outil de chiffrement (habituellement, un logiciel) pour protéger les renseignements de nature délicate avant de les transmettre à l'extérieur de l'entreprise (par exemple, dans le cas de l'envoi de pièces jointes contenant des informations confidentielles/sensibles/données à caractère personnel)?

- (0) Incertain
- (1) Non
- (2) Oui mais personne ne sait comment l'utiliser
- (3) Oui et le personnel a été formé pour l'utiliser

Pour aller plus loin :

**Entreprise 1.0**

Principe 5. Mettez votre vision en œuvre

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

Action 4. Surveillez votre environnement informatique

**Entreprise 2.0**

Principe 4. Prévoyez les dispositions en matière de protection de la vie privée

Action 7. Sauvegardez toutes les informations

Action 9. Sécurisez les postes de travail et les appareils mobiles

## 17. Votre entreprise a-t-elle mis en place une gestion (efficace) des accès aux données ?

- (0) Incertain
- (1) Non
- (2) Oui, mais concrètement tout le monde finit par avoir accès à tout
- (3) Oui et nous disposons d'un IAM : tout le monde n'a pas accès à tout

Pour aller plus loin :

**Entreprise 1.0**

Action 4. Surveillez votre environnement informatique

**Entreprise 2.0**

Action 8. Gérez les accès à vos ordinateurs et réseaux

## 18. Votre entreprise a-t-elle mis en place une formation (continue) du personnel en charge de la sécurité de l'information ?

- (0) Incertain
- (1) Non
- (2) Oui, ils se forment en interne uniquement et/ou seulement à leur arrivée
- (3) Oui et les membres du personnel concernés suivent en continu des formations internes et externes

Pour aller plus loin :

**Entreprise 1.0**

Action 3. Investissez dans la formation

**Entreprise 2.0**

Principe 2. Sensibilisez votre personnel à la sécurité de l'information

Principe 10. Prévoyez vos relations avec les tiers

Action 3. Sensibilisez vos travailleurs aux risques cyber

## 19. Votre entreprise sécurise-t-elle ses serveurs et composants réseaux de manière efficace?

- (0) Incertain
- (1) Non
- (2) Oui mais les journaux de sécurité sur les serveurs et pare-feux ne sont conservés qu'un mois et personne n'a le temps de les analyser correctement
- (3) Oui et les journaux de sécurité sur les serveurs et pare-feux sont conservés au moins 6 mois. Un système d'analyse et d'alerte (SIEM)[1] examine également ces journaux afin de détecter les comportements malveillants.

1 Voir Glossaire.

Pour aller plus loin :

**Entreprise 1.0**

Action 4. Surveillez votre environnement informatique

**Entreprise 2.0**

Principe 10. Prévoyez les relations avec les tiers

Action 4. Gérez vos ressources informatiques importantes

Action 5. Mettez à jour tous les programmes

Action 8. Gérez les accès à vos ordinateurs et réseaux

Action 10. Sécurisez les serveurs et composants réseaux

Action 11. Sécurisez les accès à distance

## 20. Votre entreprise fait-elle régulièrement évaluer la sécurité de l'information (audit de sécurité) ?

- (0) Incertain
- (1) Non
- (2) Oui mais elle n'exige rien de ses fournisseurs et personne en interne n'évalue l'utilité des informations recueillies lors des audits
- (3) Oui et l'utilité des informations recueillies est également évaluée que l'audit soit interne ou qu'il s'agisse d'un audit sur les fournisseurs

Pour aller plus loin :

**Entreprise 1.0**

Principe 4. Montrez que vous prenez vos responsabilités

Principe 5. Mettez votre vision en œuvre

**Entreprise 2.0**

Principe 5. Organisez régulièrement des tests et des contrôles

Principe 10. Prévoyez les relations avec les tiers

Action 4. Gérez vos ressources informatiques importantes

Action 8. Gérez les accès à vos ordinateurs et réseaux

**TOTAL : .....**

Vous avez terminé le questionnaire d'auto-évaluation.

Si votre résultat se situe entre 0 et 20, vous devriez lire le présent guide en entier en vous concentrant sur les points « Entreprise 1.0 » dès que possible. Assurez-vous d'avoir le soutien de votre direction et consultez d'autres personnes de l'entreprise pour commencer à y planifier et à y installer les premières mesures de cybersécurité. Ne vous découragez pas : concentrez-vous sur l'essentiel à court terme.

Si votre résultat se situe entre 20 et 40, votre entreprise a déjà réalisé certains efforts pour améliorer sa cybersécurité...mais certains pans de votre défense laissent encore à désirer. Lisez ce guide en portant une attention particulière aux domaines pour lesquels vous avez obtenu le moins de points.

Si votre résultat se situe entre 40 et 60, félicitations ! Votre entreprise a déjà accompli de nombreux progrès dans plusieurs domaines de la cybersécurité et relève de la section « Entreprise 2.0 ». Ne vous reposez cependant pas sur vos lauriers : de nouvelles menaces voient constamment le jour ! N'oubliez pas de procéder régulièrement à des audits de sécurité et de prévoir, suivant vos besoins, les prochaines étapes pour vous améliorer.