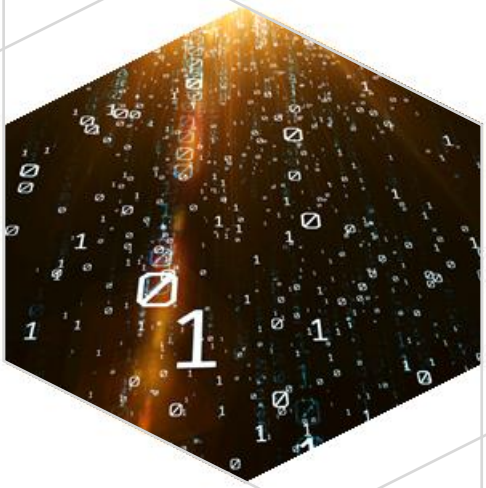
SECURITE NUMERIQUE ET CYBERSECURITE

ACCOMPAGNEMENT DES ENTREPRISES



EUROPEAN CYBER SECURITY MONTH

Nom de l'entreprise : Email :

Nom du contact : Tel :

Les questions suivantes n'ont d'autre ambition que de vous permettre de prendre un temps de réflexion sur la façon dont vous abordez la sécurité numérique au sein de votre organisation.

Ce peut être un élément complémentaire à une démarche entamée (probablement à la suite de la mise en application du RGPD voici 1 an), tout comme un moyen de compléter et/ou d'éventuellement réactiver le sujet de la sécurité numérique dans votre activité et dans son développement.

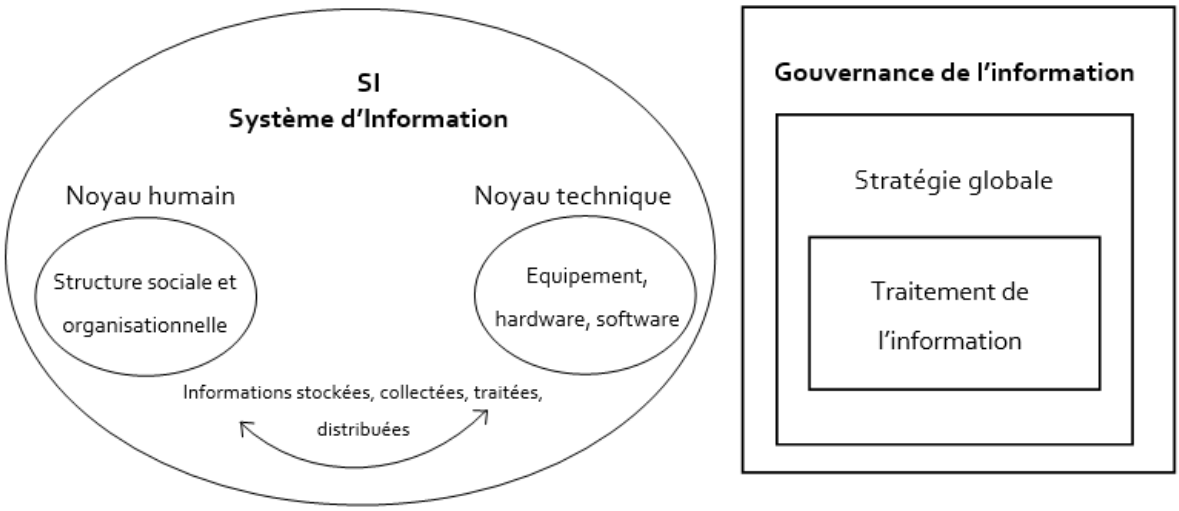
Il est important de se poser des questions mais il essentiel de savoir vers où regarder pour trouver des réponses en adéquations avec vos problématiques et à l'échelle de votre entreprise.

Par cette action, EFCSE se pose à la fois en catalyseur de réflexion et en connecteur d'information pour vous accompagner concrètement.

Préambule : de quoi parle-t-on ?

Le terme de sécurité numérique semble a priori assez descriptif pour être compréhensible, cependant, celle-ci repose sur des facteurs variés qui vont au-delà du numérique puisqu'ils concernent aussi bien des aspects physiques ou encore humains.

Dans un cadre professionnel, le numérique est aujourd'hui primordial dans le déroulement des activités des entreprises, une mauvaise gestion du sujet peut conduire à des dérives financières ou de dégradation d'un patrimoine de données, voire même à l'arrêt de l'activité.



Pour réduire les risques, le focus système d'information et gouvernance de l'information sont les ingrédients indispensables à la mise en place d'une stratégie globale optimisée

Le questionnaire suivant est à votre disposition pour creuser le sujet et , nous le souhaitons, vous permettre de placer des jalons dans votre plan numérique

C'est à vous…

.

Etape 1 : dresser un état des lieux

1. Qui est nommé officiellement responsable de la sécurité numérique dans votre entreprise ?

   ☐ Moi-même

   ☐ Responsable désigné (DSI, RSSI, …)

   ☐ Directeur (général, technique, …)

   ☐ Personne précisément

   ☐ Je n'ai pas l'information

   ☐ Autre – précisez

Être conscient du responsable de la sécurité est capital pour savoir à qui s'adresser dans l'éventualité d'une cyber attaque.

2. Que considérez-vous comme les mesures les plus importantes pour diminuer les risques de cyber attaques au sein de votre organisation ?

Niveau humain :

   ☐ Sensibilisation

   ☐ Formation

   ☐ Désignation d'un responsable de la sécurité

   ☐ Définition et/ou mise à jour des politiques/mesures de sécurité

   ☐ Autre – précisez

Niveau physique :

   ☐ Installation d'antivirus, anti-spam, anti-spyware, etc.

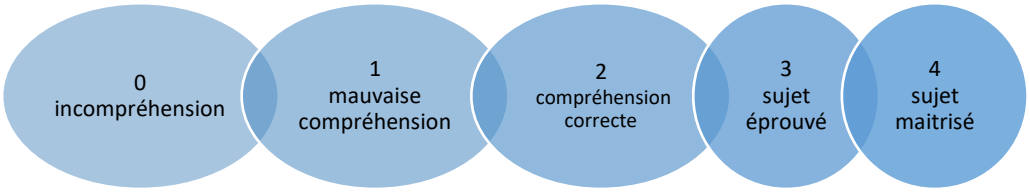
   ☐ Utilisation d'un réseau d'échanges sécurisés

   ☐ Stockage l'information chez un acteur de confiance

   ☐ Autre – précisez

Cliquez ou appuyez ici pour entrer du texte.

3. Sur le sujet de la sécurité numérique, à quel niveau de compréhension estimez-vous que les équipes se situent ?



4. Quels types d'informations votre entreprise recueille-t-elle et de quelle(s) source(s) proviennent-t-elles ?

Types d'informations

- ☐ Exclusivement lié à notre activité Administrative
- ☐ Financière (coordonnées bancaires, pièces comptables, …)
- ☐ Personnelles (clients, partenaires, …)

Sources

- ☐ Interne à l'entreprise
- ☐ Entreprises et organisations tierces
- ☐ Externes (clients, réseaux, partenaires, sous-traitants,…)
- ☐ Particuliers (clients, …)

Autre :

Recueillir des informations / données nécessite une mise en conformité / plus de détails sur ce sujet à l'étape 3.

5. Stockez-vous des données potentiellement attrayantes pour un pirate informatique ?

Particuliers :

- ☐ Nom
- ☐ Numéro de téléphone
- ☐ Adresse mail
- ☐ Adresse
- ☐ Coordonnées bancaires
- ☐ Agenda
- ☐ Consommation (carte de fidélité)
- ☐ Âge
- ☐ Niveau socio-économique
- ☐ Autres :

Professionnelle :

- ☐ Organigramme
- ☐ Listes de contacts

- ☐ Listes de prospects
- ☐ Autres :

6. Que considérez-vous être les informations les plus importantes de l'entreprise ?
   - ☐ Données des salariés
   - ☐ Données métiers
   - ☐ Eléments de stratégie (commerciale, innovation, développement international, partenariats ,…)
   - ☐ Autre

Commentaire libre :

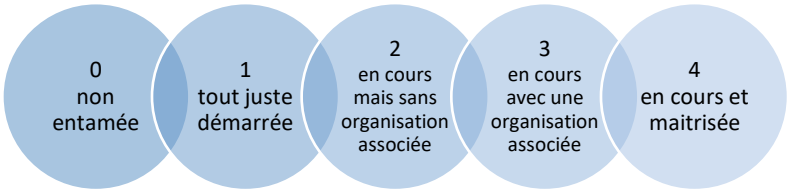
7. Comment ces informations sont-elles gérées / conservées dans votre organisation ?
   - ☐ Au format tableur (fichier Excel)
   - ☐ Base de données sur un serveur / un ordinateur de l'entreprise
   - ☐ Fichiers sur des postes de collaborateurs
   - ☐ Cloud grand public (Google par exemple)
   - ☐ Cloud professionnel
   - ☐ Hébergement en Data Centre dédié/sécurisé
   - ☐ Supports externes (disque dur, clé USB, …)

Autre ou commentaire libre :

8. Estimez-vous que l'organisation de l'entreprise vous permette de trouver rapidement la bonne information (pertinence, correspondance immédiate avec le besoin, actualisée, etc…) ?
   - ☐ Oui
   - ☐ Non

Quel serait votre conseil sur ce point ?

9. Sur une échelle de 0 à 4, où situez-vous actuellement votre démarche de transformation numérique ?



10. Selon vous, « transformation numérique » et « transition numérique » correspondent-t-elles sensiblement à la même chose ?

☐ Oui

☐ Non

Que diriez-vous en complément ?

Etape 2 : que se passe-t-il en cas d'attaque ?

Préambule : que signifie exactement que d'être attaqué ?

Une cyber attaque se traduit par une action malveillante ayant un impact sur vos activités numériques.

Ces attaques peuvent être par exemple (non exhaustif) :

- Accès à vos systèmes / appareils limité ou bloqué,
- Modification, endommagement, destruction ou vol de vos données,
- Usurpation d'identité,
- …

Elles peuvent se présenter sous formes de (non exhaustif) :

- Email frauduleux,
- Piratage de données,
- Intrusion, malwares,
- …

La matrice ci-dessous décrit quelques scénarios où une vulnérabilité pourrait se transformer en menace.

Threat Matrix						
Scenarios						
Threat\Vulnerability	Physical Physical security	Digital firewall	 antivirus	 Database	Human Personnel	Exterior forces Internet services / Wireless
Hardware theft	Insufficient on-premises access	x	x	x	x	x
Ransomware	x	Incompetent or outdated firewalls	x	Non-secured databases	x	x
Malware/virus	x	x	Incompetent or outdated antiviruses		Downloading infected files	x
Phishing	x	x	x	x	Entering personal/ financial information	x
Data leak	Inadapted storing devices (ex USB key)	x	x	Penetrable databases	Losing USB keys	Inadapted exchange services

Être conscient des causes et des conséquences des différents types d'attaques que vous pourrez rencontrer vous permettra d'être mieux préparé dans l'éventualité d'en subir une, notamment en :

- Révisant votre stratégie de sécurité,
- Définissant une politique de sécurité adéquate et adaptée à votre organisation,
- Estimant les dépenses engagées en cas d'attaque pour un réajustement éventuel du budget.

« Mieux vaut prévenir que guérir », n'attendez pas qu'il soit trop tard pour vous questionner sur les mesures à mettre en place et les bonnes pratiques à suivre lors d'une attaque.

1. Quelle est la personne qui gère les situations de crise / les cyber attaques ? Qui est son remplaçant en cas d'absence ?
   - ☐ Moi-même
   - ☐ Responsable désigné (RSSI, DSI, …)
   - ☐ Directeur (DG, …)
   - ☐ Personne précisément
   - ☐ Je n'ai pas l'information
   - ☐ Autre, précisez

N'attendez pas une cyber attaque pour vous informer ; la préparation est tout aussi importante que la prévention.

2. Votre entreprise a-t-elle du matériel non-connecté, des sauvegardes ou tout autre Plan de Continuité d'Activité (PCA) pour la reprise d'activité ?
   - ☐ Oui
   - ☐ Non

L'absence d'un PCA peut mener au ralentissement voire à l'arrêt total de vos activités, avec des conséquences fâcheuses et des pertes substantielles pour votre organisation.

3. Connaissez-vous les procédures à suivre en cas d'attaque ou la fréquence à laquelle vous testez ces procédures ?
   - ☐ Oui
   - ☐ Non

Mettre en place des procédures c'est bien, les tester c'est indispensable pour mieux les adapter et les maitriser.

4. Quelle est votre priorité lors d'une attaque ?
   - ☐ Maintenir son activité
   - ☐ Protéger sa réputation
   - ☐ Déterminer la source de l'attaque
   - ☐ Conserver les données / informations
   - ☐ Conserver le matériel informatique
   - ☐ Autre :

Etape 3 : la mise en conformité

Préambule : qu'est-ce que la mise en conformité ?

La mise en conformité est issue de l'application du RGPD le 25 mai 2018, cela correspond à recenser, au traitement de données personnelles, à la catégorisation des données personnelles, aux objectif(s) poursuivi(s) par rapport à la collecte et au traitement de données personnelles.

La conformité des données est obligatoire, il est nécessaire de se conformer au RGPD.

1. Qui a la charge de traiter les données ?
   - ☐ Responsable interne
   - ☐ Responsable externe
2. Quelle est la circulation (provenance et destination) de l'information ?

3. Les informations / les données que vous traitez sortent-t-elles du territoire européen ?
   - ☐ Oui
   - ☐ Non
   - ☐ Partiellement
   - ☐ Je ne sais pas
4. Quelles mesures avez-vous prises pour vous conformer au RGPD ?
   - ☐ Pas encore démarré
   - ☐ Mise en place du processus pour répertorier le type de données collectées
   - ☐ Formalisation de la politique de protection des données personnelles propre à notre activité (explication sur l'utilisation des données, processus sur le consentement de la personne, etc…)
   - ☐ Formation/sensibilisation en interne
   - ☐ Désignation d'un DPO
   - ☐ Autre, précisez.

Conclusion

- Merci d'indiquer dans quels domaines vous souhaiteriez voir la sécurité numérique de votre organisation renforcée :

  ☐ Installation de protections diverses (antivirus, firewall, solutions anti-spam, etc.)

  ☐ Politique de sécurité informatique (changements de mots de passe, portabilité d'outils de travails tels que l'ordinateur ou les clés USB, etc.)

  ☐ Politique de sécurité physique (accès aux locaux, vidéosurveillance, etc.)

  ☐ Sensibilisation/formation à la sécurité numérique

  ☐ Support à la mise en application du RGPD

  ☐ Autre, précisez

- A la suite de ce questionnaire, souhaitez-vous recevoir des conseils sur des procédés à mettre en place pour améliorer votre sécurité numérique ?

  ☐ Oui, à l'adresse suivante :

  ☐ Non

L'EFCSE vous remercie de l'attention que vous portez à ce sujet et souhaite que cet exercice vous permette d'alimenter réflexion et action.