La trousse élan

Conseils d'experts pour favoriser l'accompagnement

Présenté par

ADRIQ

PROMOUVOIR • MOBILISER • ACCOMPAGNER

Avec la participation financière de

Québec

Rédigé par

EFICIO

Pierre Farley, Expert-conseil en innovation, ADRIQ &
Associé & CIO sur demande, Eficio

Propulsé par

Réseau accès pme

Éléments de base en cybersécurité : liste de 20 questions

1. CONTEXTE DE L'OUTIL

La liste de contrôle accompagne le guide dans le but de :

- **Sensibiliser :** Les questions sont conçues pour faire prendre conscience aux dirigeants des divers aspects de la cybersécurité et de l'importance de chaque mesure.
- **Évaluer :** En répondant aux questions, les dirigeants pourront identifier les lacunes dans leurs stratégies actuelles de cybersécurité.

2. COMMENT RÉPONDRE AUX QUESTIONS ?

Lorsque vous utilisez cette liste de contrôle en cybersécurité, il est crucial de noter méticuleusement les réponses fournies par les dirigeants des petites entreprises. Voici comment procéder efficacement pour garantir une évaluation précise et utile :

Notation des réponses:

- **Documentation :** En tant que conseiller, vous devriez documenter les réponses exactes données par les dirigeants. Cela vous aidera à garder une trace des informations pour des analyses futures ou pour des suivis nécessaires.

- **Évaluation de la maîtrise du sujet :** Portez une attention particulière à la manière dont les questions sont comprises et aux réponses fournies. Si un dirigeant semble maîtriser les sujets abordés, cela indique une bonne connaissance de leur infrastructure de cybersécurité. Cependant, une compréhension limitée ou des réponses vagues peuvent indiquer un besoin de sensibilisation et d'amélioration.

3. SYSTÈME DE PONDÉRATION

Pour chaque question, évaluez la réponse selon le système de pondération suivant :

- **0 = Contrôle non en place :** Choisissez cette option si aucun effort de cybersécurité correspondant à la question n'est observable ou si le dirigeant indique clairement l'absence de tels contrôles.

- **1 = Partiellement en place :** Utilisez cette notation si des efforts sont faits pour mettre en place des contrôles de cybersécurité, mais ces mesures sont incomplètes, inadéquates ou ne couvrent pas tous les aspects nécessaires.

- **2 = Contrôle en place :** Cette note indique que la mesure de cybersécurité concernée est complètement implémentée et fonctionne efficacement au sein de l'entreprise.

4. INTERPRÉTATION DES SCORES

- **Évaluation du score total :** Additionnez les scores pour obtenir un total. Ce total vous donnera une vue d'ensemble du niveau de maturité en cybersécurité de l'entreprise. Le score maximum est 40.

- **Interprétation :** Un score bas indique que l'entreprise ne possède pas les contrôles de base en matière de cybersécurité, ce qui nécessite des actions immédiates pour améliorer leur posture de sécurité. Un score élevé suggère que l'entreprise est relativement bien protégée contre les menaces courantes, bien que la cybersécurité exige une évaluation et une amélioration continues.

5. SUIVI ET ACTIONS REQUISES

- **Actions basées sur le score :** Si le score est bas, discutez des actions spécifiques à entreprendre pour renforcer les contrôles de cybersécurité. Même si le score est élevé, il est important de revoir régulièrement les mesures en place et de les mettre à jour en fonction de l'évolution des menaces.

- **Sensibilisation continue :** Encouragez les dirigeants à se tenir informés et à sensibiliser leur personnel à la cybersécurité, car cela contribue significativement à la protection de l'entreprise.

En suivant cette méthode pour répondre aux questions, vous aiderez les dirigeants à mieux comprendre leur propre niveau de sécurité et à identifier les domaines nécessitant une attention immédiate. Ce processus est conçu pour être un outil d'évaluation rapide mais efficace pour les conseillers en développement économique qui accompagnent les petites entreprises dans la gestion de leur cybersécurité.

6. EXPLICATIONS DES 20 QUESTIONS DE LA LISTE DE CONTRÔLE EN CYBERSÉCURITÉ

Voici des détails sur ce que chaque question de la liste de contrôle cherche à évaluer et pourquoi ces informations sont cruciales pour renforcer la cybersécurité dans une petite entreprise.

Ces questions sont conçues pour aider les entreprises à évaluer leur posture de cybersécurité actuelle et à identifier les domaines nécessitant une attention ou une amélioration.

7. QUESTIONNAIRE

1. **Connaissez-vous clairement les risques auxquels votre entreprise s'expose ?**

   - **Objectif :** S'assurer que les dirigeants comprennent les menaces spécifiques à leur industrie et à leur environnement opérationnel.
   - **Importance :** Une bonne compréhension des risques permet d'élaborer des stratégies de défense plus efficaces.
   - **Description :** Cette question cherche à évaluer si l'entreprise a une vision précise des menaces potentielles, qu'elles soient technologiques, humaines ou organisationnelles. Les risques peuvent inclure des cyberattaques, des erreurs humaines, des défaillances de systèmes, des non-conformités réglementaires ou le non-respect de clauses contractuelles avec des clients, pouvant entraîner des pénalités financières ou des impacts sur la réputation. Une compréhension claire de ces risques est essentielle pour protéger les actifs critiques et assurer la continuité des opérations.

Réponse : _____
Point : 0 1 2

2. Avez-vous une politique de cybersécurité en place au sein de votre entreprise ?

- **Objectif :** Vérifier l'existence de directives formelles en matière de sécurité informatique.
- **Importance :** Une politique claire définit les attentes et les procédures de sécurité pour tous les employés.
- **Description :** Cette question vise à déterminer si l'entreprise dispose d'un document formel définissant les règles, pratiques et procédures pour protéger ses informations et ses systèmes contre les menaces. Une politique de cybersécurité sert de guide pour encadrer les comportements des employés, établir les responsabilités et répondre efficacement aux incidents. Elle reflète également l'engagement de l'entreprise à gérer la sécurité de manière proactive.

Réponse : _____
Point : 0 1 2

3. Vos employés reçoivent-ils régulièrement des formations sur la sécurité informatique ?

- **Objectif :** Assurer que le personnel est au courant des meilleures pratiques et des menaces actuelles.
- **Importance :** Les employés informés sont moins susceptibles de commettre des erreurs qui pourraient compromettre la sécurité.
- **Description :** Cette question explore si l'entreprise investit dans la sensibilisation et la formation de ses employés pour les rendre capables de reconnaître et de réagir aux menaces de cybersécurité. L'humain étant souvent la plus grande faille en cybersécurité, des formations régulières permettent de réduire les erreurs humaines, comme le partage accidentel de données sensibles ou le clic sur des liens malveillants, tout en instaurant une culture de sécurité au sein de l'organisation.

Réponse : _____
Point : 0 1 2

4. Utilisez-vous des mots de passe forts et une authentification à double facteur (MFA)?

- **Objectif :** Évaluer l'implémentation de pratiques de sécurité essentielles pour sécuriser l'accès aux systèmes (tous les systèmes incluant les environnements SaaS).
- **Importance :** Les mots de passe forts et le MFA constituent une défense critique contre les accès non autorisés, réduisant considérablement les risques d'intrusion.
- **Description :** Cette question vise à comprendre si l'entreprise applique des mesures de base pour protéger ses systèmes et données. Les mots de passe forts, bien qu'importants, sont vulnérables face aux outils avancés de piratage actuels. Par exemple, un mot de passe de 8 caractères comprenant des lettres majuscules, minuscules, chiffres et symboles peut être craqué en quelques heures à quelques jours avec des systèmes de calcul modernes. Ces délais continuent de diminuer à mesure que la puissance des systèmes évolue, rendant les mots de passe seuls de moins en moins fiables. L'activation du MFA est donc indispensable pour ajouter une couche essentielle de sécurité, rendant les accès critiques beaucoup plus résistants face aux cyberattaques.

Réponse : _____
Point : 0 1 2

5. Avez-vous des mesures en place pour protéger contre les logiciels malveillants et les virus ?

- **Objectif :** Évaluer la protection contre les programmes malveillants.
- **Importance :** Prévenir les infections qui peuvent causer des dommages ou des pertes de données importantes.
- **Description :** Cette question cherche à évaluer si l'entreprise dispose de protections techniques pour prévenir les infections par des logiciels malveillants, comme les antivirus, les pares-feux, et les outils de détection de menaces. Ces mesures sont essentielles pour empêcher les intrusions qui pourraient voler des données, compromettre des systèmes ou causer des interruptions d'activité.
-

Réponse : _____
Point : 0 1 2

6. Réalisez-vous des audits de sécurité réguliers ?

- **Objectif :** Déterminer la fréquence des évaluations de sécurité par des experts.
- **Importance :** Identifier les vulnérabilités potentielles avant qu'elles ne soient exploitées.
- **Description :** Cette question met l'accent sur l'importance d'évaluer périodiquement l'efficacité des mesures de sécurité en place. Les menaces en cybersécurité évoluent constamment, et sans audits réguliers, il est difficile d'identifier les failles ou non-conformités avant qu'elles ne soient exploitées. Un audit externe, réalisé par un expert indépendant, permet d'obtenir une vision claire, neutre et professionnelle, en identifiant des vulnérabilités que l'équipe interne pourrait ne pas percevoir.

Réponse : _____
Point : 0 1 2

7. Avez-vous un plan de réponse en cas d'incident de sécurité informatique ?

- **Objectif :** Vérifier l'existence d'un plan d'action pour les incidents de sécurité.
- **Importance :** Permettre une réaction rapide et efficace en cas de problème de sécurité pour minimiser les dégâts.
- **Description :** Cette question vise à vérifier si l'entreprise dispose d'un plan écrit et structuré pour réagir efficacement en cas d'incident de cybersécurité. Un plan documenté, régulièrement révisé et mis à jour, est essentiel pour garantir une réponse rapide et coordonnée. Il permet de limiter les impacts, de rétablir les opérations rapidement et de respecter les obligations légales ou contractuelles, tout en évitant l'improvisation lors d'une crise.

Réponse : _____
Point : 0 1 2

8. Savez-vous où vos données les plus sensibles sont stockées et qui y a accès ?

- **Objectif :** S'assurer que les informations critiques sont bien protégées et que l'accès est strictement contrôlé.
- **Importance :** Prévenir les fuites de données et assurer la confidentialité des informations sensibles.
- **Description :** Cette question vise à évaluer si l'entreprise a une visibilité claire sur l'emplacement et l'accès à ses données critiques. Savoir où ces informations sont stockées et contrôler qui peut y accéder est essentiel pour réduire les risques de fuite, d'accès non autorisé ou de non-conformité réglementaire. Au Québec, cette démarche est également une exigence clé pour respecter les obligations de la Loi 25, qui renforce la protection des renseignements personnels et impose une gestion rigoureuse des données sensibles.

Réponse : _____
Point : 0 1 2

9. Avez-vous des sauvegardes régulières de vos données importantes ?

- **Objectif :** Confirmer l'existence de procédures de sauvegarde pour les données essentielles.
- **Importance :** Garantir la récupérabilité des données en cas de perte ou de corruption.
- **Description :** Cette question vise à s'assurer que l'entreprise protège ses données critiques contre les pertes potentielles causées par des cyberattaques, des erreurs humaines ou des défaillances techniques. Il est important de rappeler que même si vos données sont hébergées dans le nuage, cela ne dispense pas de réaliser des sauvegardes régulières. Une copie indépendante des données, stockée de manière sécurisée et testée périodiquement, est essentielle pour garantir leur récupération en cas d'incident majeur affectant le fournisseur de services cloud.

Réponse : _____
Point : 0 1 2

10. Vos systèmes et logiciels sont-ils régulièrement mis à jour pour corriger les failles de sécurité ?

- **Objectif :** Évaluer la gestion des mises à jour et des correctifs de sécurité.
- **Importance :** Maintenir les systèmes à l'abri des vulnérabilités connues exploitées par les cybercriminels.
- **Description :** Cette question évalue si l'entreprise maintient ses systèmes et logiciels à jour pour se protéger contre les vulnérabilités connues. Les mises à jour régulières, incluant les correctifs de sécurité, sont essentielles pour réduire les risques d'exploitation par des cyberattaques. Ignorer ces mises à jour expose l'entreprise à des menaces évitables et peut compromettre la stabilité et la sécurité de ses infrastructures.

Réponse : _____
Point : 0 1 2

11. Avez-vous des contrôles d'accès en place pour limiter qui peut voir et utiliser certaines informations ?

- **Objectif :** Examiner les mesures de contrôle d'accès aux données.
- **Importance :** Assurer que seules les personnes autorisées ont accès à des informations spécifiques.
- **Description :** Cette question vise à vérifier si l'entreprise applique des mesures pour restreindre l'accès aux données et systèmes sensibles uniquement aux personnes autorisées. Des contrôles d'accès bien définis, basés sur les rôles et les responsabilités, réduisent les risques d'accès non autorisé, d'abus ou de fuite de données. Cela inclut des pratiques comme le principe du moindre privilège et l'utilisation d'outils de gestion des identités et des accès.

Réponse : _____
Point : 0 1 2

12. Utilisez-vous le chiffrement pour protéger les données sensibles ?

- **Objectif :** Vérifier l'usage du chiffrement pour sécuriser les données.
- **Importance :** Protéger l'intégrité et la confidentialité des données, surtout lors de la transmission ou du stockage.
- **Description :** Cette question vise à déterminer si l'entreprise applique le chiffrement comme mesure essentielle pour protéger les données sensibles, que ce soit lors de leur stockage ou de leur transmission. Le chiffrement des courriels, par exemple, est une pratique cruciale pour garantir que les informations envoyées ne puissent pas être interceptées ou lues par des tiers non autorisés. Cela renforce la confidentialité des communications, particulièrement lorsque des renseignements sensibles ou confidentiels sont échangés. Avez-vous des mesures de sécurité pour votre réseau Wi-Fi d'entreprise ?

Réponse : _____
Point : 0 1 2

13. Avez-vous des mesures de sécurité pour votre réseau Wi-Fi d'entreprise ?

- **Objectif :** S'assurer que le réseau sans fil est sécurisé contre les intrusions.
- **Importance :** Prévenir les accès non autorisés au réseau interne de l'entreprise.
- **Description :** Cette question vise à évaluer si le réseau Wi-Fi de l'entreprise est protégé contre les accès non autorisés et les cyberattaques. Des mesures de sécurité telles que le chiffrement (WPA3 recommandé), l'utilisation de mots de passe complexes, la segmentation des réseaux (par exemple, un réseau distinct pour les invités) et le contrôle des appareils connectés sont essentielles pour garantir la confidentialité et la sécurité des données transmises sur le réseau.

Réponse : _____
Point : 0 1 2

14. Vos employés utilisent-ils des appareils mobiles ou laptop pour accéder aux ressources de l'entreprise ? Si oui, ces appareils sont-ils sécurisés ?

- **Objectif :** Évaluer la sécurité des appareils mobiles utilisés pour le travail.
- **Importance :** Protéger les points d'entrée mobiles qui pourraient être exploités pour accéder à des ressources d'entreprise.
- **Description :** Cette question vise à évaluer si l'entreprise sécurise l'utilisation des appareils mobiles et portables pour accéder à ses systèmes ou données. Ces appareils, souvent utilisés hors des environnements contrôlés, présentent des risques accrus d'accès non autorisé, de vol ou de perte de données. La mise en place de mesures de sécurité comme le chiffrement des données, des mots de passe forts, des logiciels de protection, la gestion des appareils mobiles (MDM) et l'utilisation de réseaux sécurisés (VPN) est essentielle pour protéger les ressources de l'entreprise.

Réponse : _____
Point : 0 1 2

15. Comment gérez-vous les accès des anciens employés à vos systèmes informatiques ?

- **Objectif :** Assurer que les anciens employés n'ont plus accès aux systèmes et données de l'entreprise.
- **Importance :** Éviter les risques de sécurité liés à des comptes non désactivés.
- **Description :** Cette question vise à déterminer si l'entreprise dispose d'un processus clair pour révoquer rapidement les accès aux systèmes et données lorsqu'un employé quitte l'organisation. Une gestion rigoureuse des accès des anciens employés est essentielle pour éviter tout risque d'accès non autorisé, d'abus ou de fuite de données après leur départ. Cela inclut la désactivation des comptes, la récupération des appareils et le suivi des autorisations résiduelles dans les systèmes tiers.

Réponse : _____
Point : 0 1 2

16. Avez-vous des politiques en place pour la sécurité des courriels et éviter les tentatives de phishing ?

- **Objectif :** Confirmer l'existence de politiques pour sécuriser les communications par courriel et sensibiliser contre le phishing.
- **Importance :** Réduire le risque d'hameçonnage, une des cyberattaques les plus courantes.
- **Description :** Cette question cherche à évaluer si l'entreprise a mis en place des règles et des pratiques pour protéger les communications par courriel contre les cyberattaques, notamment le phishing. Les politiques peuvent inclure la sensibilisation des employés, l'utilisation de filtres anti-phishing, l'authentification des courriels (DMARC, SPF, DKIM) et des procédures pour signaler les courriels suspects. Une telle approche réduit les risques de compromission et protège les données sensibles échangées par courriel.

Réponse : _____
Point : 0 1 2

17. Utilisez-vous un pare-feu ou d'autres technologies pour protéger votre réseau ?

- **Objectif :** Identifier les mesures de protection du réseau en place.
- **Importance :** Prévenir les accès non autorisés et surveiller les activités suspectes sur le réseau.
- **Description :** Cette question vise à vérifier si l'entreprise utilise des outils comme des pare-feu pour protéger son réseau contre les intrusions, les attaques et les activités suspectes. Les pare-feu, combinés à d'autres technologies comme les systèmes de détection et de prévention des intrusions (IDS/IPS), les VPN ou les réseaux segmentés, jouent un rôle essentiel en surveillant et en contrôlant le trafic entrant et sortant, garantissant ainsi une sécurité renforcée pour l'infrastructure réseau.

Réponse : _____
Point : 0 1 2

18. Comment assurez-vous la sécurité de vos transactions en ligne ou de votre commerce électronique ?

- **Objectif :** Examiner les pratiques de sécurité pour les transactions en ligne.
- **Importance :** Protéger contre la fraude et sécuriser les échanges financiers en ligne.
- **Description :** Cette question vise à évaluer les mesures mises en place pour protéger les transactions en ligne et les données des clients. Cela inclut l'utilisation de protocoles sécurisés comme HTTPS, le chiffrement des informations sensibles (ex. : données bancaires), des outils de détection de fraude, et la conformité aux normes de sécurité telles que PCI-DSS. Une sécurité rigoureuse est essentielle pour renforcer la confiance des clients et prévenir les cyberattaques comme le vol de données ou les fraudes.

Réponse : _____
Point : 0 1 2

19. Avez-vous un responsable dédié à la gestion de la cybersécurité au sein de votre entreprise ?

- **Objectif :** S'assurer de l'existence d'un rôle assigné à la surveillance et la gestion de la cybersécurité.
- **Importance :** Avoir une personne responsable permet une meilleure coordination et mise en œuvre des politiques de sécurité (imputabilité).
- **Description :** Cette question vise à déterminer si l'entreprise a désigné une personne ou une équipe spécifique pour superviser et gérer la cybersécurité. Un responsable de la cybersécurité, comme un CISO (Chief Information Security Officer), est essentiel pour élaborer des stratégies, gérer les risques et coordonner les réponses aux incidents. Pour les entreprises qui n'ont pas les moyens ou le besoin d'un CISO à temps plein, il est possible d'opter pour un service de CISO virtuel à temps partiel. Ce type de service offre une expertise stratégique et opérationnelle adaptée aux besoins spécifiques de l'entreprise, tout en optimisant les coûts.

Réponse : _____
Point : 0 1 2

20. Comment évaluez-vous et gérez-vous les risques de cybersécurité liés à vos fournisseurs et partenaires externes ?

- **Objectif :** Contrôler comment les risques externes sont gérés.
- **Importance :** Assurer que les tiers respectent également des normes de sécurité adéquates pour protéger vos données et celles de vos clients.
- **Description :** Cette question vise à comprendre si l'entreprise prend en compte les risques de cybersécurité associés à ses fournisseurs et partenaires externes. Ces derniers peuvent représenter une menace si leurs systèmes ou pratiques de sécurité sont insuffisants. Une gestion proactive inclut des évaluations régulières, des clauses contractuelles de sécurité, et des audits ou certifications pour s'assurer qu'ils respectent les normes nécessaires. La collaboration avec des tiers ne devrait jamais compromettre la sécurité globale de l'entreprise.

Réponse : _____
Point : 0 1 2

ADRIQ

2025

La trousse élan

Conseils d'experts pour favoriser l'accompagnement