CYBER-SÉCURITÉ POUR LES ORGANISATIONS PLUS PETITES

LISTE DE CONTRÔLE DU PDG : LEADERSHIP DE LA CYBER-SÉCURITÉ

GOUVERNANCE

- ☐ **Nommer un responsable de la sécurité des systèmes d'information (RSSI) s'il n'y en a pas.**
- ☐ **Établir et maintenir une politique de cyber-sécurité à l'échelle de l'organisation, basée sur les risques et informée par les normes et directives internationales, nationales et industrielles.**
- ☐ **Définir les rôles et responsabilités de tous les membres du personnel impliqués dans la cyber-sécurité. Travailler avec votre RSSI pour identifier les rôles de cyber-sécurité et les droits d'accès appropriés pour tous les niveaux de personnel.**
- ☐ **Établir ou identifier des canaux de communication clairs entre les unités distinctes ou les membres du personnel qui traitent les différents aspects de la cyber-sécurité.**
- ☐ **Vous assurer que le RSSI dispose d'une ligne de communication claire et directe pour vous signaler les menaces en temps opportun, ainsi qu'au conseil d'administration.**
- ☐ **Inviter régulièrement votre RSSI ou autres membres du personnel technique pour informer la haute direction.**
- ☐ **Vérifier que les politiques, normes et mécanismes de cyber-sécurité sont uniformes dans l'ensemble de l'organisation.**

ÉVALUATION ET GESTION DES RISQUES

- ☐ **Effectuer une évaluation des risques de cyber-sécurité en collaboration avec votre RSSI ou un autre membre du personnel technique, qui doit inclure de :**
  - Décrire les actifs de votre organisation et leurs différents niveaux de dépendance technologique ;
  - Évaluer la maturité de votre organisation et les risques inhérents associés aux dépendances technologiques de ses actifs ;
  - Déterminer l'état de maturité souhaité de votre organisation ;
  - Comprendre où les menaces de cyber-sécurité s'inscrivent dans la liste des priorités de risque de votre organisation ;
  - Identifier les écarts entre votre état actuel de cyber-sécurité et l'état cible souhaité ;
  - Mettre en œuvre des plans pour atteindre et maintenir la maturité ;
  - Évaluez et affectez des fonds pour investir dans la sécurité et corriger les écarts existants,
  - Réévaluer continuellement la maturité, les risques et les objectifs de cyber-sécurité de votre organisation ; et
  - Envisager des mesures de protection telles que l'achat d'une cyber-assurance.
- ☐ **Analyser et présenter les résultats aux principales parties prenantes et au conseil.**
- ☐ **Prévoir de superviser les étapes pour améliorer la préparation en matière de cyber-sécurité et suivre la progression.**

CULTURE ORGANISATIONNELLE

- ☐ **Discuter régulièrement des cyber-risques et de la sécurité au niveau de la direction.**
- ☐ **S'assurer que la formation sur la cyber-sécurité fait partie de l'intégration de tous les employés et faire signer à tous les employés les documents indiquant qu'ils acceptent de respecter les politiques de cyber-sécurité de l'organisation.**
- ☐ **Établir une formation récurrente à la cyber-sécurité pour tout le personnel.**
- ☐ **S'assurer de toujours tenir compte de la cyber-sécurité lorsque l'organisation évalue les fournisseurs potentiels et partage des données avec des tiers.**
- ☐ **Intégrez une évaluation de la cyber-sécurité d'une organisation en tenant compte des fusions et acquisitions.**
- ☐ **Instaurer un examen annuel des politiques de cyber-sécurité de l'organisation.**
- ☐ **Encourager le personnel technique à s'engager dans le partage volontaire des informations sur les menaces et incidents de cyber-sécurité.**

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

SWIFT INSTITUTE

FS-ISAC

Standard Chartered

CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE

ICBA
Independent Community Bankers of America®