CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

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

PRINCIPES FONDAMENTAUX DE LA GOUVERNANCE DES CYBER-RISQUES

- ☐ En tant que groupe, évaluez régulièrement si le conseil peut répondre de manière affirmative aux questions suivantes :
  - Votre organisation a-t-elle satisfait aux exigences légales et réglementaires pertinentes, par exemple au RGPD ?
  - Votre organisation a-t-elle quantifié ses cyber-expositions et testé sa résilience financière ?
  - Votre organisation a-t-elle un plan d'amélioration en place pour garantir que les expositions s'inscrivent dans votre appétit au risque convenu ?
  - Le conseil discute-t-il régulièrement des informations concises, claires et exploitables relatives à la cyber-résilience de l'organisation et fournies par la direction ?
  - Votre organisation a-t-elle des plans de réponse aux incidents en place qui ont récemment été testés, y compris au niveau du conseil ?
  - Les rôles des personnes clés responsables de la gestion des cyber-risques sont-ils clairs et alignés sur les trois lignes de défense ?
  - Avez-vous obtenu une validation et une assurance indépendantes de la posture de cyber-sécurité de votre organisation, par exemple, via des tests, une certification ou une assurance ?
- ☐ Si vous ne pouvez pas répondre de manière affirmative à un ou plusieurs des éléments ci-dessus, travaillez avec votre PDG, le RSSI, le personnel de l'organisation concerné et/ou des ressources externes pour résoudre le problème.

SUPERVISION

- ☐ Assurez-vous que le conseil d'administration est conscient de son rôle de responsable ultime pour le cyber-risque et la résilience de votre organisation.
  - ☐ Déléguez la supervision à un comité du conseil spécifique si nécessaire.
- ☐ Assignez à un responsable de l'entreprise, généralement le responsable de la sécurité des systèmes d'information (RSSI), la responsabilité de signaler la capacité de votre organisation à gérer la cyber-résilience et les progrès dans la mise en œuvre des objectifs de cyber-résilience.
  - ☐ Assurez-vous que ce responsable dispose d'un accès régulier au conseil d'administration, d'une autorité suffisante, de la maîtrise du sujet, de l'expérience et des ressources pour remplir ces obligations.
- ☐ Définissez annuellement la tolérance au risque de votre organisation, en assurant la cohérence avec votre stratégie d'entreprise et l'appétit au risque.
- ☐ Assurez-vous qu'un examen formel et indépendant de la cyber-résilience de votre organisation est effectué chaque année.
- ☐ Travaillez pour intégrer la cyber-résilience et l'évaluation des risques dans la stratégie commerciale globale de votre organisation, la gestion des risques, la budgétisation et l'allocation des ressources.
- ☐ Supervisez la création, la mise en œuvre, les tests et l'amélioration continue des plans de cyber-résilience, en vous assurant qu'ils sont harmonisés dans l'ensemble de votre organisation et que votre RSSI ou autre cadre responsable les signale régulièrement au conseil d'administration.
- ☐ Passez régulièrement en revue vos performances pour ce qui précède et tenez compte des conseils indépendants pour une amélioration continue.

RESTER INFORME

- ☐ Lorsqu'une personne rejoint le conseil, assurez-vous qu'elle dispose des compétences et connaissances appropriées et actualisées pour comprendre et gérer les risques posés par les cyber-menaces.
- ☐ Sollicitez des conseils réguliers de la part de la direction sur l'exposition au risque actuelle et future de votre organisation, les exigences réglementaires pertinentes, et les références du secteur et de la société pour l'appétit au risque. Prévoyez de participer :
  - aux séances d'information régulières sur les obligations créées par les nouvelles réglementations et législations ;
  - à la planification commune du conseil et du comité de direction et aux visites aux pairs et aux leaders de la meilleure pratique en matière de cyber-sécurité ;
  - aux séances d'information relatives à la sécurité sur l'environnement des menaces ; et
  - aux échanges au niveau du conseil des informations sur la gouvernance et les rapports.
- ☐ Indiquez clairement à la direction qu'elle a la responsabilité de signaler une évaluation quantifiée et compréhensible des cyber-risques, menaces et événements comme un élément permanent à l'ordre du jour lors des réunions du conseil d'administration.
- ☐ Vérifiez régulièrement auprès de la direction et des autres membres du personnel concernés, les développements liés aux problèmes systémiques constants tels que les vulnérabilités de la chaîne d'approvisionnement, les dépendances courantes et l'écart dans le partage des informations entre les tableaux sur la gouvernance des cyber-risques.

DONNER LE TON

- ☐ Assurez-vous que les membres du personnel, à tous les niveaux, reconnaissent qu'ils ont chacun des responsabilités importantes pour garantir la cyber-résilience de votre organisation.
- ☐ Supervisez le rôle de la direction dans la promotion et le maintien de la culture du risque de votre organisation. Évaluez régulièrement l'efficacité de la culture du risque de votre organisation, en tenant compte de l'impact de la culture sur la sécurité et la solidité, et en apportant des changements si nécessaire.
- ☐ Indiquez clairement que vous attendez de tout le personnel qu'il agisse avec intégrité et qu'il fasse remonter rapidement le non-respect observé au sein ou à l'extérieur de votre organisation.

CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

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

GOUVERNANCE

- ☐ Nommez un responsable de la sécurité des systèmes d'information (RSSI) s'il n'y en a pas.
- ☐ Établissez 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.
- ☐ Définissez 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.
- ☐ Établissez 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.
- ☐ Assurez-vous 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.
- ☐ Invitez régulièrement votre RSSI ou autres membres du personnel technique pour informer la haute direction.
- ☐ Vérifiez 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 ;
  - 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.
- ☐ 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.

CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

LISTE DE CONTRÔLE DU RSSI : PROTÉGER VOTRE ORGANISATION

DEVELOPPER UN PROGRAMME DE SECURITÉ DES INFORMATIONS BASÉ SUR LES RISQUES

- ☐ Identifiez et énumérez tous les types d'informations que votre entreprise stocke ou utilise (par ex., noms des clients et e-mails).
- ☐ Interrogez et enregistrez les réponses pour chaque type d'information :
  - Que se passerait-il si ces informations étaient rendues publiques ?
  - Qu'adviendrait-il de mon entreprise si ces informations étaient incorrectes ?
  - Qu'adviendrait-il de mon entreprise si je/mes clients n'avaient pas pu accéder à ces informations ?
- ☐ Enregistrez la technologie en contact avec les informations que vous avez identifiées. Cela peut inclure du matériel (par ex., ordinateurs) et des applications logicielles (par ex., e-mail du navigateur).
  - Le cas échéant, incluez des technologies externes à votre entreprise (par ex., « le cloud ») et toutes les technologies de protection que vous avez en place, telles que les pare-feu.
  - Incluez la marque, le modèle, les numéros de série et les autres identifiants.
  - Trouvez où se trouve chaque produit. Pour le logiciel, identifiez la ou les machines sur lesquelles le logiciel a été chargé.
- ☐ Examinez régulièrement les menaces et vulnérabilités que le secteur financier peut rencontrer et estimez la probabilité que vous soyez affecté auprès de votre CERT national, FS-ISAC, votre section InfraGard local, etc.
- ☐ Effectuez une analyse des vulnérabilités au moins une fois par an.
- ☐ Créez une politique de cyber-sécurité pour votre organisation.
- ☐ Formez tous les employés sur les détails de la politique et demandez-leur de signer des documents attestant de leur rôle dans le maintien permanent de la cyber-sécurité de votre organisation en respectant la politique.

PRÉVENIR LES DOMMAGES LIÉS AUX LOGICIELS MALVEILLANTS

- ☐ Activez votre pare-feu et définissez des listes de contrôle d'accès (ACL). Limitez l'accès en utilisant un paramètre de liste blanche.
- ☐ Utilisez un logiciel antivirus et un logiciel anti-espion sur tous les ordinateurs et ordinateurs portables.
- ☐ Appliquez les dernières mises à jour logicielles fournies par les fabricants et les fournisseurs. « Mettez à jour automatiquement », le cas échéant.
- ☐ Limitez l'installation de nouveaux programmes au personnel informatique avec des droits d'administrateur.
- ☐ Conservez et surveillez les journaux d'activité générés par le matériel ou le logiciel de protection/détection. Protégez les journaux avec une protection par mot de passe et un chiffrement des mots de passe.
- ☐ Assurez-vous que toutes les horloges hôtes sont synchronisées.
- ☐ Contrôlez l'accès aux supports amovibles tels que les cartes SD et les clés USB. Encouragez le personnel à transférer des fichiers par e-mail ou par stockage cloud. Informez le personnel sur les risques liés à l'utilisation de clés USB provenant de sources externes ou à la transmission de leurs clés USB à d'autres personnes.
- ☐ Configurez la sécurité de la messagerie et les filtres de courrier indésirable sur vos services de messagerie.

- ☐ Protégez toutes les pages de vos sites Web publics avec les outils de chiffrement et les autres outils disponibles.
- ☐ Envisagez d'embaucher un service de test d'intrusion pour évaluer la sécurité des actifs et des systèmes de votre organisation.

FORMER LES EMPLOYÉS

- ☐ Planifiez d'effectuer des formations obligatoires sur la cyber-sécurité lors de l'intégration des nouveaux employés et à intervalles réguliers pour tous les employés actuels, au moins une fois par an. Exigez des employés :
  - qu'ils utilisent des mots de passe forts sur tous les appareils et comptes professionnels et encouragez-les à faire de même pour leurs appareils personnels et à utiliser un gestionnaire de mots de passe ;
  - qu'ils maintiennent tous les systèmes d'exploitation, logiciels et applications à jour sur tous les appareils ;
  - qu'ils utilisent une authentification à deux facteurs sur tous les comptes ;
  - qu'ils conservent les détails des comptes et les cartes d'accès en sécurité et verrouillent les appareils lorsqu'ils ne les utilisent pas ;
  - qu'ils s'abstiennent de partager les détails des comptes ou d'autres données sensibles via un e-mail non chiffré ou d'autres communications ouvertes ;
  - qu'ils évitent d'ouvrir automatiquement des pièces jointes ou de cliquer sur des liens dans des e-mails non sollicités ou suspects ;
  - qu'ils vérifient la validité d'un e-mail suspect ou d'une fenêtre contextuelle avant de fournir des informations personnelles, et qu'ils accordent une attention particulière à l'adresse e-mail ; et
  - qu'ils signalent tout incident de sécurité interne ou externe potentiel, menace ou mauvaise manipulation des données ou des appareils au personnel technique de votre organisation et/ou aux cadres supérieurs.
- ☐ Programmez et réalisez des tests réguliers sur la sensibilisation des employés à travers des problèmes simulés, par exemple en envoyant des e-mails de style hameçonnage à partir de faux comptes. Évaluez les défaillances des employés et utilisez-les comme des opportunités d'apprentissage et d'amélioration.

PROTÉGER VOS DONNÉES

- ☐ Effectuez des sauvegardes régulières de vos données importantes (par ex., documents, e-mails, calendriers) et vérifiez qu'elles peuvent être restaurées. Envisagez de sauvegarder sur le cloud.
- ☐ Assurez-vous que l'appareil contenant votre sauvegarde n'est pas connecté de façon permanente à l'appareil qui détient la copie originale, ni physiquement ni via un réseau local.
- ☐ Installez des protecteurs de surtension, utilisez des générateurs et assurez-vous que tous vos ordinateurs et périphériques réseau critiques sont branchés sur des alimentations sans interruption.
- ☐ Utilisez une solution de gestion des appareils mobiles (MDM - Mobile Device Management).

SÉCURISER VOS APPAREILS

- ☐ Activez la protection par code PIN ou mot de passe pour les appareils mobiles. Configurez les appareils pour que, lorsqu'ils sont perdus ou volés, ils puissent être suivis, vidés à distance ou verrouillés à distance.
- ☐ Gardez vos appareils (et toutes les applications installées) à jour, en utilisant l'option « Mettre à jour automatiquement » si disponible.

- ☐ Lorsque vous envoyez des données sensibles, ne vous connectez pas aux points d'accès Wi-Fi publics ; utilisez des connexions cellulaires (y compris des dongles de connexion sans fil) ou utilisez des VPN.
- ☐ Remplacez les appareils qui ne sont plus pris en charge par les fabricants par des solutions alternatives à jour.
- ☐ Définissez des procédures de signalement pour les équipements perdus ou volés.

UTILISER DES MOTS DE PASSE

- ☐ Assurez-vous que tous les ordinateurs utilisent des produits de chiffrement qui nécessitent un mot de passe pour démarrer. Activez la protection par mot de passe ou code PIN pour les appareils mobiles.
- ☐ Utilisez des mots de passe forts, en évitant les mots de passe prévisibles (comme m0tdepasse) et les identifiants personnels (comme les noms de famille et d'animaux). Demandez à tous les employés de faire de même.
- ☐ Utilisez l'authentification à deux facteurs (2FA) dans la mesure du possible.
- ☐ Modifiez les mots de passe par défaut émis par le fabricant sur tous les appareils, y compris les périphériques réseau et IoT, avant de les distribuer au personnel.
- ☐ Assurez-vous que le personnel peut réinitialiser facilement ses propres mots de passe. Vous pouvez également demander aux employés de modifier leur mot de passe à intervalles réguliers (par ex., trimestriel, semestriel ou annuel).
- ☐ Envisagez d'utiliser un gestionnaire de mots de passe. Si vous en utilisez un, assurez-vous que le mot de passe « maître » (qui fournit l'accès à tous vos autres mots de passe) est un mot de passe fort.

CONTRÔLER LES AUTORISATIONS

- ☐ Assurez-vous que tous les employés disposent de comptes identifiables uniques qui sont authentifiés chaque fois qu'ils accèdent à vos systèmes.
- ☐ Donnez uniquement des privilèges administratifs à un personnel informatique et un personnel clé fiables et révoquez les privilèges d'administrateur sur les postes de travail pour les utilisateurs standard.
- ☐ Donnez uniquement aux employés l'accès aux systèmes de données spécifiques dont ils ont besoin pour leur travail et assurez-vous qu'ils ne peuvent installer aucun logiciel sans autorisation.
- ☐ Créez des comptes utilisateur pour chaque employé sur les ordinateurs de votre organisation.

SÉCURISER VOTRE WI-FI

- ☐ Assurez-vous que votre Wi-Fi professionnel est sécurisé et chiffré avec WPA2. Les routeurs sont souvent fournis avec le chiffrement désactivé, alors assurez-vous de l'activer. Protégez l'accès au routeur par un mot de passe et assurez-vous que le mot de passe est mis à jour à partir de la valeur par défaut prédéfinie. Désactivez les fonctions de « gestion à distance ».
- ☐ Configurez votre point d'accès sans fil ou votre routeur afin qu'il ne diffuse pas le nom du réseau, appelé Identificateur SSID (Service Set Identifier).
- ☐ Limitez l'accès à votre réseau Wi-Fi en autorisant uniquement les périphériques avec certaines adresses de contrôle d'accès aux médias. Si des clients ont besoin de Wi-Fi, configurez un réseau public distinct.
- ☐ Activez la connexion DHCP (Dynamic Host Configuration Protocol) sur vos périphériques réseau afin de faciliter le suivi de tous les périphériques qui se sont connectés à votre réseau.

- ☐ Déconnectez-vous en tant qu'administrateur après avoir configuré le routeur.
- ☐ Gardez le logiciel de votre routeur à jour. Enregistrez votre routeur auprès du fabricant et inscrivez-vous pour obtenir les mises à jour.

ÉVITER LES ATTAQUES PAR HAMEÇONNAGE

- ☐ Assurez-vous que le personnel ne navigue pas sur le Web ou vérifiez les e-mails sur les serveurs ou à partir d'un compte avec des privilèges d'administrateur.
- ☐ Configurez les filtres Web et de messagerie. Pensez à empêcher les employés de visiter des sites Web fréquemment associés aux menaces de cyber-sécurité.
- ☐ Apprenez aux employés à détecter des signes évidents d'hameçonnage, comme l'orthographe et la grammaire médiocres, ou des versions de logos reconnaissables de mauvaise qualité. L'adresse e-mail de l'expéditeur semble-t-elle légitime ?
- ☐ Effectuez une analyse anti-logiciels malveillants et modifiez les mots de passe dès que possible si vous soupçonnez une attaque. Ne punissez pas les employés s'ils sont victimes d'une attaque par hameçonnage (cela dissuade les personnes de signaler les problèmes par la suite).

CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

LISTE DE CONTRÔLE DU RSSI : PROTÉGER VOS CLIENTS

CONSEILLER LES CLIENTS ET LES EMPLOYÉS SUR LA PROTECTION DES DONNÉES AU NIVEAU INDIVIDUEL

☐ Fournissez aux employés et aux clients les recommandations personnelles suivantes à respecter pour mieux protéger leurs données :

- Utilisez des mots de passe forts sur tous les appareils personnels et professionnels, et envisagez d'utiliser un gestionnaire de mots de passe.
- Gardez les systèmes d'exploitation et autres logiciels et applications à jour sur vos ordinateurs et appareils mobiles.
- Installez des logiciels antivirus, anti-logiciels malveillants et anti-ransomware qui empêchent, détectent et éliminent les programmes malveillants.
- Utilisez un programme pare-feu pour empêcher l'accès non autorisé à votre ordinateur.
- Utilisez uniquement des produits de sécurité d'entreprises réputées. Lisez les commentaires des publications d'ordinateurs et de consommateurs et envisagez de consulter le fabricant de votre ordinateur ou système d'exploitation.
- Soyez prudent avec les informations sensibles. N'envoyez pas de mots de passe de compte bancaire ou d'autres données de comptes financiers sensibles via un e-mail non chiffré.
- Soyez intelligent quant à l'endroit et à la manière dont vous vous connectez à Internet pour les services bancaires ou autres communications impliquant des informations personnelles sensibles.
- N'ouvrez pas automatiquement les pièces jointes des e-mails ou ne cliquez pas sur des liens dans des e-mails non sollicités ou suspects. Arrêtez-vous. Réfléchissez. Cliquez.
- Méfiez-vous si quelqu'un vous contacte soudainement en ligne ou par téléphone et vous demande vos informations personnelles. Même lorsque vous communiquez avec des adresses connues, essayez de réduire au minimum le partage d'informations personnelles par e-mail.
- N'oubliez pas qu'aucun établissement financier ne vous enverra un courrier électronique ou ne vous appellera et ne vous demandera des informations confidentielles qu'ils ont déjà vous concernant.
- Partez du principe qu'une demande d'information d'une banque où vous n'avez jamais ouvert un compte est une arnaque.
- Vérifiez la validité d'un e-mail suspect ou d'une fenêtre contextuelle avant de fournir des informations personnelles. Accordez une attention particulière à l'adresse e-mail.

ADMINISTRER DES COMPTES

☐ Exigez que les clients utilisent des identifiants et des mots de passe forts pour se connecter à vos services. Recommandez-leur de ne pas utiliser un mot de passe déjà utilisé pour d'autres comptes.

☐ Utilisez la vérification instantanée, la vérification en temps réel, la vérification de dépôt d'essai, la vérification d'identité et/ou des questions à réponses ouvertes pour valider les clients réels et réduire l'opportunité de fraude.

☐ Proposez ou, idéalement, exigez l'utilisation de l'authentification à deux facteurs pour les clients lorsqu'ils se connectent à vos services.

☐ Vérifiez régulièrement les comptes des utilisateurs pour détecter des signes de fraude.

PROTÉGER LES DONNÉES

- ☐ Déterminez les données clients que votre organisation doit collecter pour exécuter ses services, et soyez prudent si vous collectez des données clients qui vont au-delà.
- ☐ Définissez et distribuez des politiques de conservation des données. Supprimez les données clients lorsqu'elles ne sont plus nécessaires.
- ☐ Chiffrez les données clients en transit et au repos.
- ☐ Mettez en place des politiques de sécurité des données pour indiquer clairement quelles méthodes de transfert de données sont approuvées par rapport aux restrictions et pour spécifier ce qui est acceptable pour tous les employés lorsqu'ils traitent des données clients. Veillez à ce que ces politiques soient documentées, communiquées, appliquées pour tous les employés, et régulièrement examinées et mises à jour.

SÉCURISER DES APPLICATIONS WEB PUBLIQUES

- ☐ Appliquez le protocole HTTPS sur les applications Web publiques de votre organisation et redirigez tout le trafic HTTP vers HTTPS.
- ☐ Utilisez une politique de sécurité du contenu sur votre ou vos sites Web.
- ☐ Activez l'épinglage de clé publique sur votre ou vos sites Web.
- ☐ Assurez-vous que votre ou vos applications Web publiques n'utilisent jamais les cookies pour stocker des informations très sensibles ou critiques sur le client (comme les mots de passe) et qu'elles disposent de dates d'expiration conservatrices pour les cookies (mieux vaut tôt que tard).
- ☐ Pensez à chiffrer les informations stockées dans les cookies que vous utilisez.
- ☐ Envisagez d'embaucher un service de test d'intrusion pour évaluer la sécurité de votre ou vos applications Web publiques au moins une fois par an.

FORMER LES EMPLOYÉS

- ☐ Responsabilisez vos employés et apprenez-leur les stratégies pour minimiser l'erreur humaine qui pourrait exposer les données clients. Cela implique de leur recommander de :
    - Minimiser leur accès et la transmission des données clients à seulement ce qui est nécessaire pour exécuter leur travail ;
    - Maintenir des pratiques de sécurité solides sur tous les appareils et comptes qui traitent des données clients en utilisant des mots de passe forts, en activant l'authentification à deux facteurs, en gardant les logiciels à jour et en ne cliquant pas sur des liens suspects ; et
    - Signaler tout incident de sécurité interne ou externe potentiel, menace ou mauvaise manipulation des données du client au personnel technique de votre organisation et/ou aux cadres supérieurs.
- ☐ Assurez-vous que vos employés comprennent et ont signé des documents pour adhérer aux politiques de protection des données et de sécurité de votre organisation.

INFORMER LES CLIENTS

- ☐ Sensibilisez à l'environnement réglementaire de votre organisation en matière de gestion des violations de données clients afin de vous assurer que vous êtes prêt à vous y conformer en cas d'incident.
- ☐ Lorsque votre organisation prend connaissance d'un incident d'accès non autorisé à des informations sensibles du client, enquêtez pour déterminer rapidement la probabilité que les informations aient été ou seront mal utilisées. Suivez les bonnes pratiques de notification et informez le ou les clients concernés dès que possible avec :
  - Une description générale de l'incident et des informations qui ont été violées ;
  - Un numéro de téléphone pour plus d'informations et pour obtenir une assistance ;
  - Un rappel pour « rester vigilant » au cours des 12 à 24 prochains mois ;
  - Une recommandation de signalement rapide des incidents d'usurpation d'identité suspectée ;
  - Une description générale des mesures prises par l'établissement financier afin de protéger les informations d'un accès ou d'une utilisation non autorisé(e) ;
  - Les coordonnées des agences d'évaluation de crédit ; et
  - Toute autre information requise par les réglementations avec lesquelles votre organisation doit se conformer.

CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

LISTE DE CÔNTROLE DU RSSI : PROTÉGER LES CONNEXIONS À DES TIERS

CHOISIR DES FOURNISSEURS EN GARDANT A L'ESPRIT LA CYBER-SÉCURITÉ

Chaque fois que vous évaluez un fournisseur potentiel, passez en revue les questions suivantes :

- ☐ A-t-il déjà servi des clients similaires à votre organisation ?
- ☐ A-t-il documenté leur conformité aux normes de cyber-sécurité connues (comme le cadre NIST ou ISO 27001, ou peut-il fournir un rapport SOC2) ?
- ☐ Parmi vos données et/ou actifs, auxquels aura-t-il besoin d'accéder pour effectuer son service et demande-t-il un accès apparemment inutile ?
- ☐ Comment prévoit-il de protéger les actifs et les données de votre organisation en sa possession ?
- ☐ Comment gère-t-il ses propres cyber-risques tiers et peut-il fournir des informations sur la sécurité de sa chaîne d'approvisionnement ?
- ☐ Quel est son plan pour la reprise après sinistre et la continuité des activités en cas d'incident impactant votre organisation ?
- ☐ Comment maintiendra-t-il votre organisation à jour en termes de communication des tendances, menaces et changements au sein de son organisation ?

IDENTIFIER LE RISQUE PAR LE BIAIS DE TIERS

Effectuez une évaluation des cyber-risques tiers, en incluant les étapes suivantes :

- ☐ Créez et mettez constamment à jour une liste de toutes les relations avec les fournisseurs et les actifs et données exposés dans chacun d'eux.
- ☐ Examinez les données auxquelles a accès chaque fournisseur ou tiers, en vérifiant que chaque niveau d'accès respecte le principe du « privilège minimum ».
- ☐ Classez vos relations fournisseurs et tiers (faible, moyen, élevé) sur la base de l'impact qu'une violation de leurs systèmes aurait sur votre organisation.
- ☐ En commençant par les fournisseurs les plus à risque, évaluez les capacités de cyber-sécurité de chaque fournisseur et la conformité aux normes pertinentes.
- ☐ Élaborez un plan pour une évaluation régulière de la sécurité, en gardant à l'esprit que vous pouvez vouloir mener occasionnellement des évaluations sur site des fournisseurs présentant le plus haut risque et/ou un accès plus important aux données clients.

GÉRER LA SÉCURITÉ DES TIERS

- ☐ Effectuez une vérification approfondie. Établissez des attentes en matière de cyber-sécurité dans les demandes de proposition, les contrats, la continuité d'activité, la réponse aux incidents et les contrats de niveau de service avec les fournisseurs. Convenez des responsabilités et obligations en cas de cyber-incident.
- ☐ Renseignez-vous sur les pratiques en matière de cyber-sécurité des organisations financières et des autres entités avec lesquelles vous effectuez des transactions ou des partages de données, en gardant à l'esprit que vos fournisseurs et tiers doivent également respecter les mêmes exigences de cyber-sécurité que celles que votre organisation doit respecter.
- ☐ Utilisez les mesures établies et convenues pour surveiller la conformité de vos fournisseurs avec les normes de cyber-sécurité.
- ☐ Vérifiez auprès de vos fournisseurs qui traitent des données sensibles s'ils proposent l'authentification à deux facteurs, le chiffrement ou d'autres mesures de sécurité pour tous les comptes dont vous disposez.

- ☐ Assurez-vous que tous les logiciels et matériels tiers que vous installez disposent d'un protocole de transfert de sécurité de sorte que les processus de démarrage soient sécurisés via des codes d'authentification et ne s'exécutent pas si les codes ne sont pas reconnus.
- ☐ Si vous rencontrez des produits de fournisseur qui sont contrefaits ou ne correspondent pas aux spécifications, travaillez pour négocier une résolution ou une stratégie de sortie.
- ☐ Évaluez annuellement les contrats des fournisseurs et assurez-vous qu'ils continuent à répondre à vos exigences stratégiques et aux exigences de sécurité des données réglementaires. Lors de la résiliation du contrat, incluez des stipulations vous permettant de récupérer vos actifs ou données et de vérifier que les actifs ou les données sont entièrement effacés du côté du fournisseur, et désactivez tout accès à vos systèmes ou serveurs.

PARTAGER DES INFORMATIONS

- ☐ Assurez-vous de disposer de canaux de communication clairs et de points de contact pour communiquer sur les problèmes de sécurité avec les fournisseurs et les homologues de votre organisation.
- ☐ Assurez-vous d'avoir des procédures en place pour garantir un partage opportun des informations de cyber-sécurité fiables et exploitables avec les parties prenantes internes et externes (y compris les entités et les autorités publiques au sein et en dehors du secteur financier).
- ☐ Suivez les mises à jour pertinentes sur les expériences des autres organisations avec leurs tiers en termes de menaces, vulnérabilités, incidents et réponses en faisant partie des organisations qui partagent des informations, comme FS-ISAC, et en cherchant d'autres sources d'informations sur les menaces.

CYBER-SÉCURITÉ POUR LES PETITES ORGANISATIONS FINANCIÈRES

LISTE DE CONTRÔLE EN CAS D'INCIDENT

PRÉPARATION

- ☐ Travaillez avec la haute direction de votre organisation et les autres membres du personnel concernés pour développer un plan de réponse aux incidents et de continuité d'activité basé sur les risques les plus pressants qui ont été identifiés dans l'évaluation des cyber-risques de votre organisation.
  - ☐ Développez des scénarios de menaces pour les types d'incidents liés aux cyber-risques prioritaires de votre organisation. Concentrez-vous sur le renforcement des capacités à réagir à ces scénarios.
  - ☐ Identifiez, enregistrez et mettez à disposition, dans votre organisation, une liste des points de contact pour une réponse aux incidents.
  - ☐ Identifiez et enregistrez les coordonnées des agences de lutte contre la fraude et des fonctionnaires locaux et fédéraux.
  - ☐ Établissez des dispositions précisant quels types d'incidents doivent être signalés, quand ils doivent être signalés, et à qui.
  - ☐ Établissez des directives écrites qui décrivent la rapidité à laquelle le personnel doit réagir à un incident et quelles mesures doivent être prises, en fonction des facteurs pertinents tels que l'impact fonctionnel et d'information de l'incident, et la capacité de récupération probable de l'incident.
  - ☐ Informez tous les employés de contacter votre équipe technique – le plus souvent, ce sera le personnel informatique et/ou le RSSI/DSI/autre responsable équivalent, lorsqu'un incident se produit.
  - ☐ Déployez des solutions pour surveiller les actions des employés et permettre l'identification des menaces et incidents d'initiés.
  - ☐ Incluez des plans de continuité d'activité pour coordonner la manière dont votre organisation travaillera avec les fournisseurs et les clients principaux pendant une urgence professionnelle, y compris la manière dont vous mèneriez des opérations professionnelles manuelles ou alternatives, si nécessaire.
  - ☐ Incluez les procédures écrites pour l'arrêt et le redémarrage du système d'urgence.
  - ☐ Développez et testez des méthodes de récupération et de restauration des données de sauvegarde ; testez régulièrement les données de sauvegarde pour vérifier leur validité.
  - ☐ Disposez d'accords et de procédures établis pour mener des opérations professionnelles sur une autre installation/un autre site.
    Disposez d'un canal de diffusion clair pour tous les clients.
  - ☐ Développez et testez des méthodes de récupération et de restauration des données de sauvegarde ; testez régulièrement les données de sauvegarde pour vérifier leur validité.
  - ☐ Disposez d'accords et de procédures établis pour mener des opérations professionnelles sur une autre installation/un autre site.
  - ☐ Disposez d'un canal de diffusion clair pour tous les clients.

PRATIQUER

- ☐ Organisez de petits exercices avec tous les membres du personnel ou représentants de tous les niveaux du personnel, y compris les cadres de l'organisation, le personnel des relations publiques/de la communication, ainsi que les équipes juridiques et de conformité.
- ☐ Identifiez et idéalement participez à des exercices sectoriels pertinents pour votre organisation.
- ☐ Établissez un processus pour garantir que les enseignements tirés des exercices sont intégrés et traités dans la stratégie de cyber-sécurité de votre entreprise.

APPORTER UNE RÉPONSE

- ☐ Mettez en œuvre des actions du plan de réponse aux incidents afin de minimiser l'impact sur les opérations professionnelles.
- ☐ Identifiez les systèmes affectés/compromis et évaluez les préjudices.
- ☐ Réduisez les préjudices en éliminant (déconnectant) les actifs concernés.
- ☐ Commencez à enregistrer toutes les informations dès que l'équipe soupçonne qu'un incident s'est produit. Tentez de conserver des preuves de l'incident lors de la déconnexion/séparation d'un actif identifié comme étant affecté ; par exemple, collectez les journaux de la configuration du système, du réseau et de la détection d'intrusion à partir des actifs affectés.
- ☐ Informez les parties internes appropriées, les fournisseurs tiers et les autorités, et demandez de l'aide si nécessaire.
- ☐ Initiez des activités de notification et d'assistance client conformément aux lois, réglementations et directives inter-agences.
- ☐ Utilisez des plateformes de partage des menaces telles que FS-ISAC ou MISP pour informer le secteur de la menace.
- ☐ Documentez toutes les étapes qui ont été prises pendant l'incident pour un examen ultérieur.

RÉCUPÉRATION

- ☐ Restaurez les actifs récupérés à des « points de récupération » périodiques si disponibles et utilisez les données de sauvegarde pour restaurer les systèmes au dernier état « correct » connu.
- ☐ Créez des sauvegardes « propres » actualisées des actifs restaurés et assurez-vous que toutes les sauvegardes des actifs critiques sont stockées dans un emplacement sécurisé physiquement et de manière écologique.
- ☐ Testez et vérifiez si les systèmes infectés sont entièrement restaurés. Confirmez que les systèmes affectés fonctionnent normalement.

RÉVISION

- ☐ Menez une discussion « enseignements tirés » après l'incident : rencontrez les cadres dirigeants, les conseillers de confiance et le(s) fournisseur(s) d'assistance informatique pour examiner les vulnérabilités possibles ou recommander de nouvelles étapes à mettre en œuvre.
- ☐ Si possible, identifiez les vulnérabilités (que ce soit dans les logiciels, le matériel, les opérations professionnelles ou le comportement du personnel) qui ont conduit à l'incident, puis élaborez un plan pour les prévenir.
- ☐ Confirmez que les systèmes affectés fonctionnent normalement.
- ☐ Élaborez un plan de surveillance pour détecter des incidents similaires ou supplémentaires liés aux problèmes identifiés.
- ☐ Partagez les enseignements tirés et les informations sur l'incident sur les plateformes de partage des menaces telles que FS-ISAC.
- ☐ Intégrez les enseignements tirés dans les protocoles de réponse aux incidents de votre organisation.