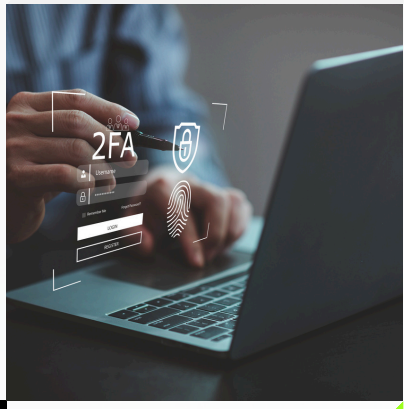
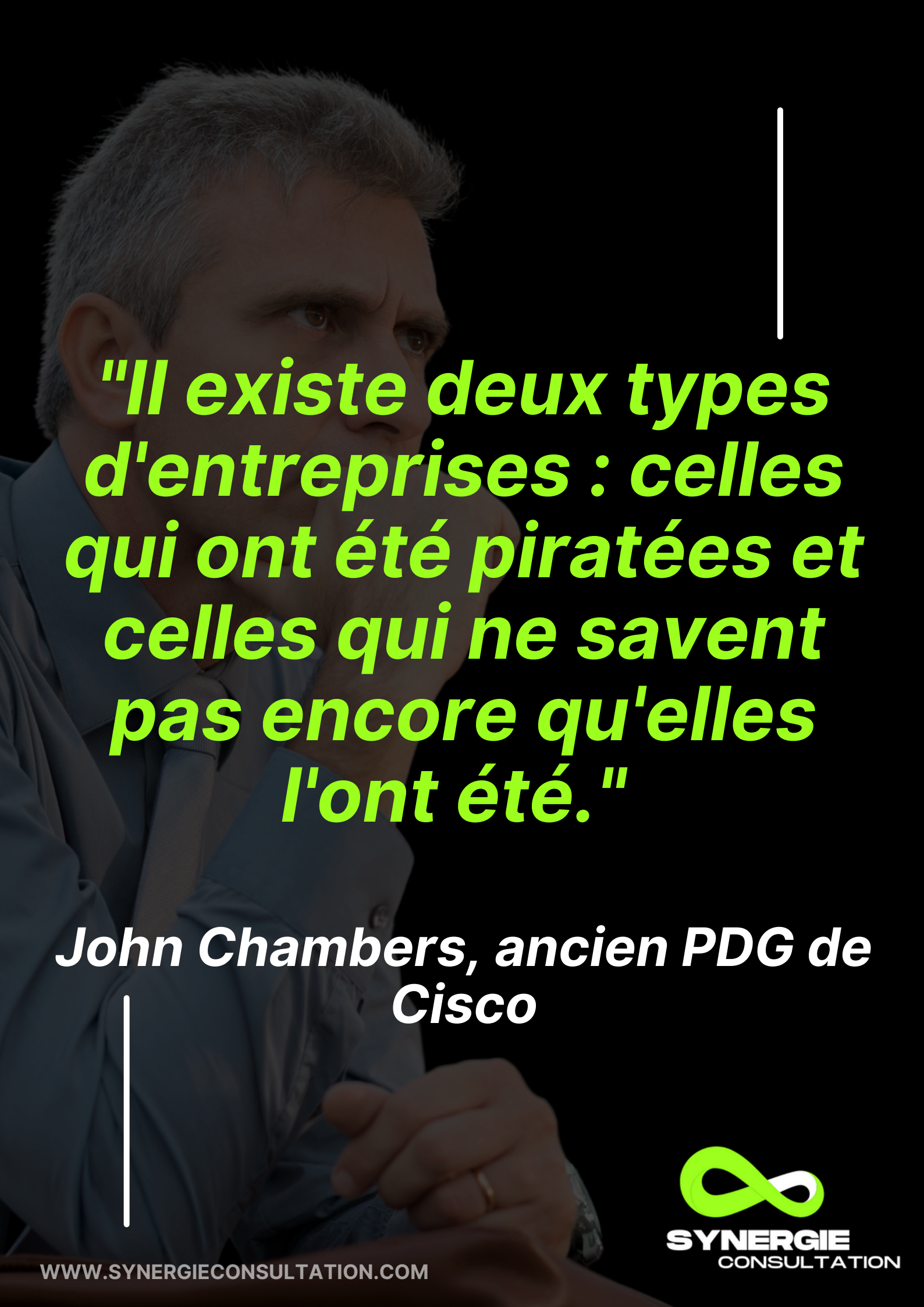
Sécurité de l'information pour les PME

Un guide pratique pour protéger votre entreprise face aux cybermenaces!



SYNERGIE
CONSULTATION

SYNERGIE
CONSULTATION



"Il existe deux types d'entreprises : celles qui ont été piratées et celles qui ne savent pas encore qu'elles l'ont été."

John Chambers, ancien PDG de Cisco

SYNERGIE CONSULTATION

WWW.SYNERGIECONSULTATION.COM

Introduction

LA SÉCURITÉ DE L'INFORMATION (SI) N'EST PAS UN LUXE, MAIS UNE NÉCESSITÉ POUR VOTRE PME.

"Dans un monde où les attaques deviennent de plus en plus sophistiquées, ***chaque PME doit agir pour protéger ses données et sa réputation.***

Ce document offre aux PME des ***pratiques et stratégies éprouvées pour renforcer leur SI.*** *Destiné aux dirigeants de la SI, il vise à préparer les entreprises* ***à faire face aux menaces et à instaurer une culture de SI durable.****"*

"Le FBI rapporte qu'en 2023, il a reçu plus de 22 000 plaintes relatives à la compromission de courriers électroniques professionnels, avec des pertes de plus de 2,9 milliards USD"

Source

Engagement de la direction

Pour que la SI devienne une priorité dans votre PME, il est essentiel que **la direction s'engage dans la création d'une culture de la SI.** Cet engagement ce traduit par

01 **La nomination d'un responsable de la SI et l'octroi de ressources.**

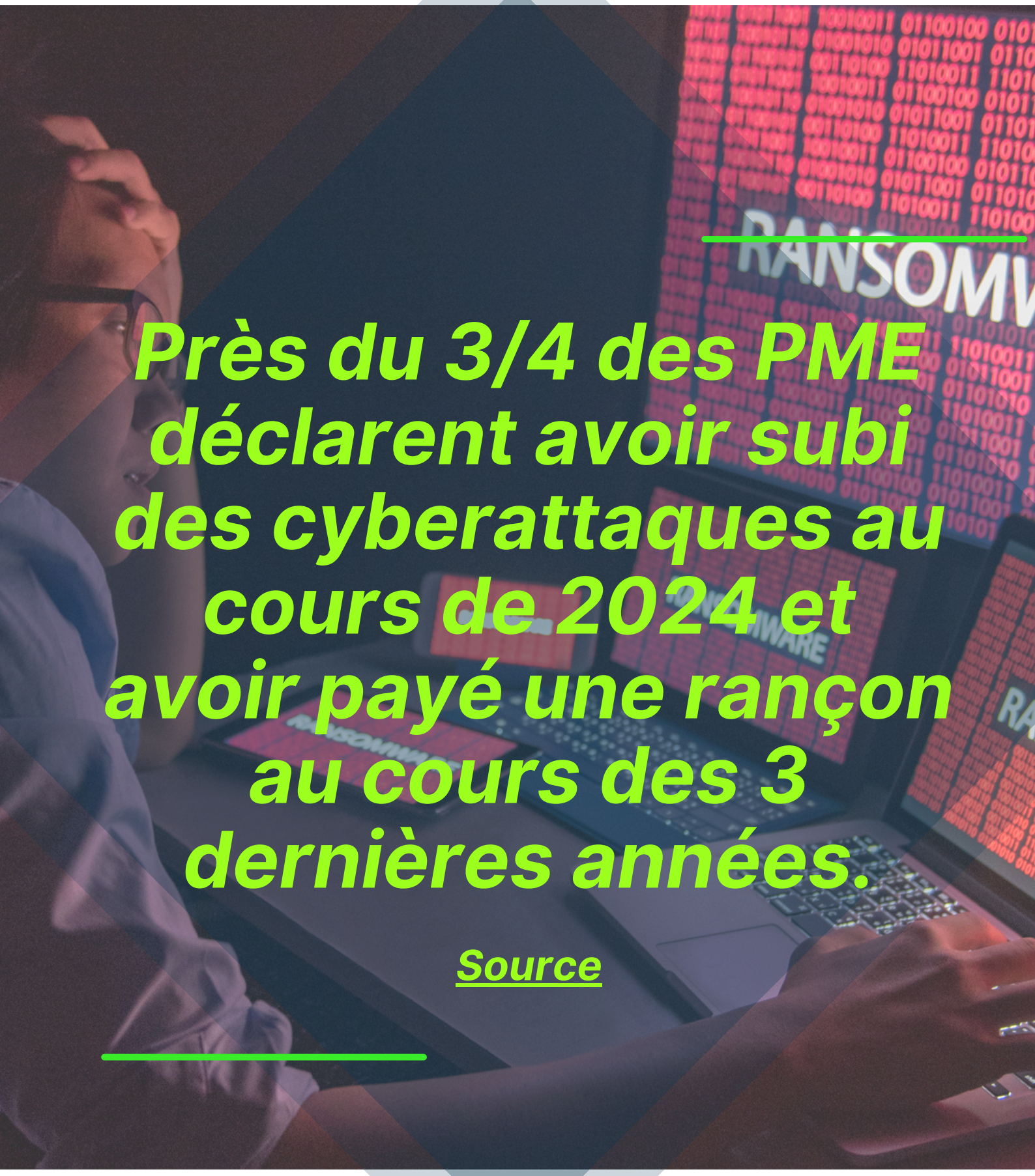
02 L'élaboration d'une **politique de sécurité et l'intégration de la SI** dans les **objectifs stratégiques.**

03 **La mise en place d'une stratégie de communication en SI** incluant des sessions de formation.

04 **L'intégration de la SI dans les pratiques quotidiennes** permettant de réduire les risques et incidents de SI.

En 2021, seulement 26 % des entreprises canadiennes avaient des politiques en matière de sécurité.

Source



Près du 3/4 des PME déclarent avoir subi des cyberattaques au cours de 2024 et avoir payé une rançon au cours des 3 dernières années.

Source

SYNERGIE CONSULTATION

Gestion des **risques** et **classification**

La gestion des risques et la classification de l'information sont des éléments essentiels permettant de protéger les actifs informationnels (AI) de votre entreprise.

En gérant vos risques, vous vous protégez **contre les cyberattaques et vous renforcez votre résilience organisationnelle.**

IDENTIFICATION DES ACTIFS INFORMATIONNELS

Avant de mettre en place des mesures de sécurité, vous devez **connaitre chacun de vos AI**

CLASSIFICATION

Une fois les AI identifiés, il faut classifier les informations selon qu'elles sont **publiques, internes, confidentielles ou critiques** afin de les protéger selon le niveau de classification.

GESTION ET ÉVALUATION DES RISQUES

L'évaluation des risques permet de **comprendre les menaces** qui pèsent sur vous et **prioriser les mesures de protection**.

En suivant un cadre d'évaluation reconnu (ex. ISO 27005) vous pouvez réaliser une analyse de risques structurée rapidement.

La gestion des accès

La gestion des accès permet de minimiser vos risques!

PRINCIPE DU MOINDRE PRIVILÈGE

Accordez aux utilisateurs uniquement les accès dont ils ont besoin pour accomplir leurs tâches en fonction des besoins d'affaires.

AUTHENTIFICATION MULTI-FACTEURS (MFA)

Utilisez le MFA pour renforcer la sécurité des connexions. Elle ajoute une couche de protection supplémentaire en exigeant un autre facteur d'authentification en plus du mot de passe.

RÉVISION DES ACCÈS

Mettez en place des audits permettant de vérifier que les accès attribués sont toujours justifiés.

SYNERGIE CONSULTATION

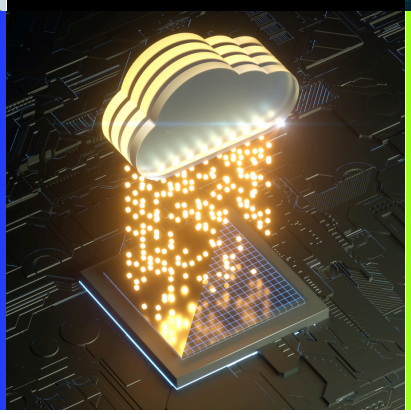
L’exploitation au quotidien de la sécurité de l’information

Appliquer les correctifs régulièrement

Détecter les menaces

Sensibiliser en continu les utilisateurs

Sauvegarder les données régulièrement et tester le plan de reprise



Contrôler et gérer les accès

"L’exploitation de la SI au quotidien **nécessite de la rigueur, repose sur des pratiques constantes** et sur la **responsabilisation de chaque utilisateur** garantissant une protection continue des actifs de l'entreprise!"

SYNERGIE CONSULTATION

Les sauvegardes et la continuité

UN PLAN DE CONTINUITÉ EST ESSENTIEL POUR RÉDUIRE AU MINIMUM LE RISQUE D'UNE SITUATION D'URGENCE COMME UNE CYBERATTAQUE.

SOURCE

DE PLUS EN PLUS DE CYBERATTAQUES VISENT LES COPIES DE SAUVEGARDE EMPÊCHANT LES ENTREPRISES DE RESTAURER LEURS DONNÉES.

CETTE TENDANCE DÉMONTRE LA NÉCESSITÉ DE MAINTENIR DES COPIES HORS LIGNE POUR UNE PLUS GRANDE RÉSILIENCE.

SOURCE

PLAN DE SAUVEGARDE RÉGULIER

Mettez en place des sauvegardes automatiques selon la règle du 3-2-1 (3 copies, 2 types de stockage et 1 hors site) et effectuez-les fréquemment.

TEST DE RESTAURATION

Organisez des tests de restauration réguliers afin de vérifier l'intégrité des copies et vous assurer que les données peuvent être récupérées.

STOCKAGE HORS LIGNE ET COPIES MULTIPLES

En plus des sauvegardes en ligne, conservez des copies hors ligne pour vous protéger. Des versions multiples dans divers emplacements réduisent les risques de perte de données.

PLAN DE CONTINUITÉ DES AFFAIRES

Élaborez un plan précisant les étapes en cas de sinistre. Ce plan doit inclure les responsabilités, les procédures de reprise et les contacts pour une récupération rapide.

SYNERGIE CONSULTATION

La **surveillance continue**

La surveillance continue est un pilier de la SI permettant de détecter et de répondre rapidement aux menaces.

Voici les éléments clés d'une surveillance efficace.

- **METTRE EN PLACE UN SYSTÈME DE DÉTECTION DES MENACES.**
- **AUTOMATISER CERTAINES TÂCHES ET UTILISER L'IA.**
- **RÉVISER RÉGULIÈREMENT LES JOURNAUX ET ANALYSER LES INFORMATIONS.**
- **FORMER VOS ÉQUIPES EN CONTINU.**
- **SUIVRE VOS INDICATEURS DE SÉCURITÉ.**

21%

Selon une enquête de Statistique Canada de 2021, 21 % des entreprises canadiennes ont déclaré avoir été touchées par des incidents de sécurité. **Une proportion significative d'entre elles n'avait pas mis en place de mesures de surveillance continue.**

La **formation** et la **sensibilisation**

Une formation régulière en SI permet de **sensibiliser les utilisateurs face aux risques, aux tendances et de les équiper afin de répondre efficacement aux événements de sécurité.**

Voici les éléments clés pour structurer une stratégie de formation solide.

01

SENSIBILISATION DE BASE

Commencez par une formation obligatoire sur les bases de la SI, comme le phishing, les bonnes pratiques de mots de passe et la protection des appareils personnels.

02

FORMATION CONTINUE

Mettez en place des sessions régulières de sensibilisation permettant de tenir les employés informés des nouvelles menaces et techniques d'attaque. **Incluez des cas pratiques et des exemples récents.**

03

FORMATION SPÉCIALISÉE

Offrez des formations approfondies et spécialisées pour les employés occupant des postes stratégiques et à haut risque.

04

ÉVALUATION ET SUIVI

Mettez en place des évaluations des compétences en SI. De petits tests après chaque session permettent de s'assurer que les connaissances sont acquises et d'ajuster le contenu.

Une stratégie de formation bien conçue fait de chaque employé un acteur clé de la sécurité, augmentant la vigilance et la réactivité de votre PME face aux menaces.

SYNERGIE
CONSULTATION

Une vision innovante en action!

À propos de nous

Chez Synergie Consultation nous transformons la manière dont les entreprises abordent la sécurité de l'information et les bonnes pratiques en TI.

Notre vision

Nous aspirons à être la référence pour les PME en développant vos compétences vous permettant de relever les défis actuels et futurs en SI et en TI.

Nos services

- Planification en sécurité
- Service en gouvernance
- Analyse de risques
- Service d'audits
- Gestion des risques liés aux tiers
- Création de politiques, normes et directives
- Accompagnement de projet
- Évaluation de votre posture de sécurité
- Service de RSI (CISO) à la demande

Contactez-nous

SERVICES@SYNERGIECONSULTATION.COM

Références

01 Small Business Cybersecurity Corner

02 Le paysage changeant de la cybersécurité

03 ENISA Threat Landscape 2024

04 La cybersécurité

05 Veeam révèle que 93 % des cyberattaques ciblent les sauvegardes

06 Modèle de plan de continuité

Synergie Consultation
Version : 1.0
Date : 27-11-2024

SYNERGIE CONSULTATION