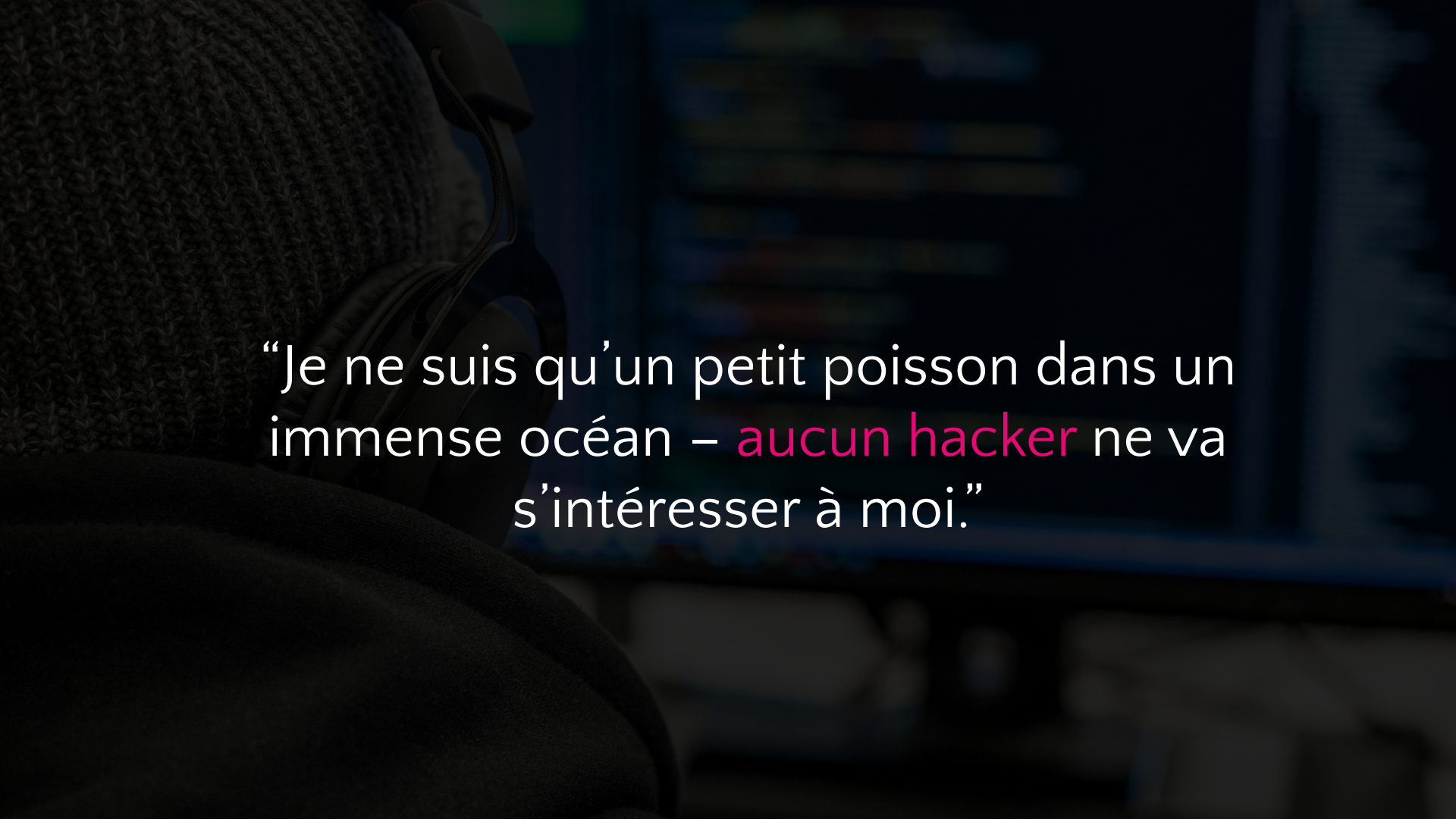
LA BRASSERIE DU DIGITAL

Table ronde
Cybersécurité

B&C informatique

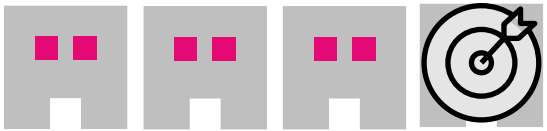
Animé par
Laurent & Nicolas

strat &SI


“Je ne suis qu’un petit poisson dans un immense océan – aucun hacker ne va s’intéresser à moi.”

Les cyberciminels ciblent les entreprises de toutes tailles

Une sur quatre est une PME [1]



24% les données clients sont atteintes
20% les données des ventes sont volées

Perte moyenne [2]

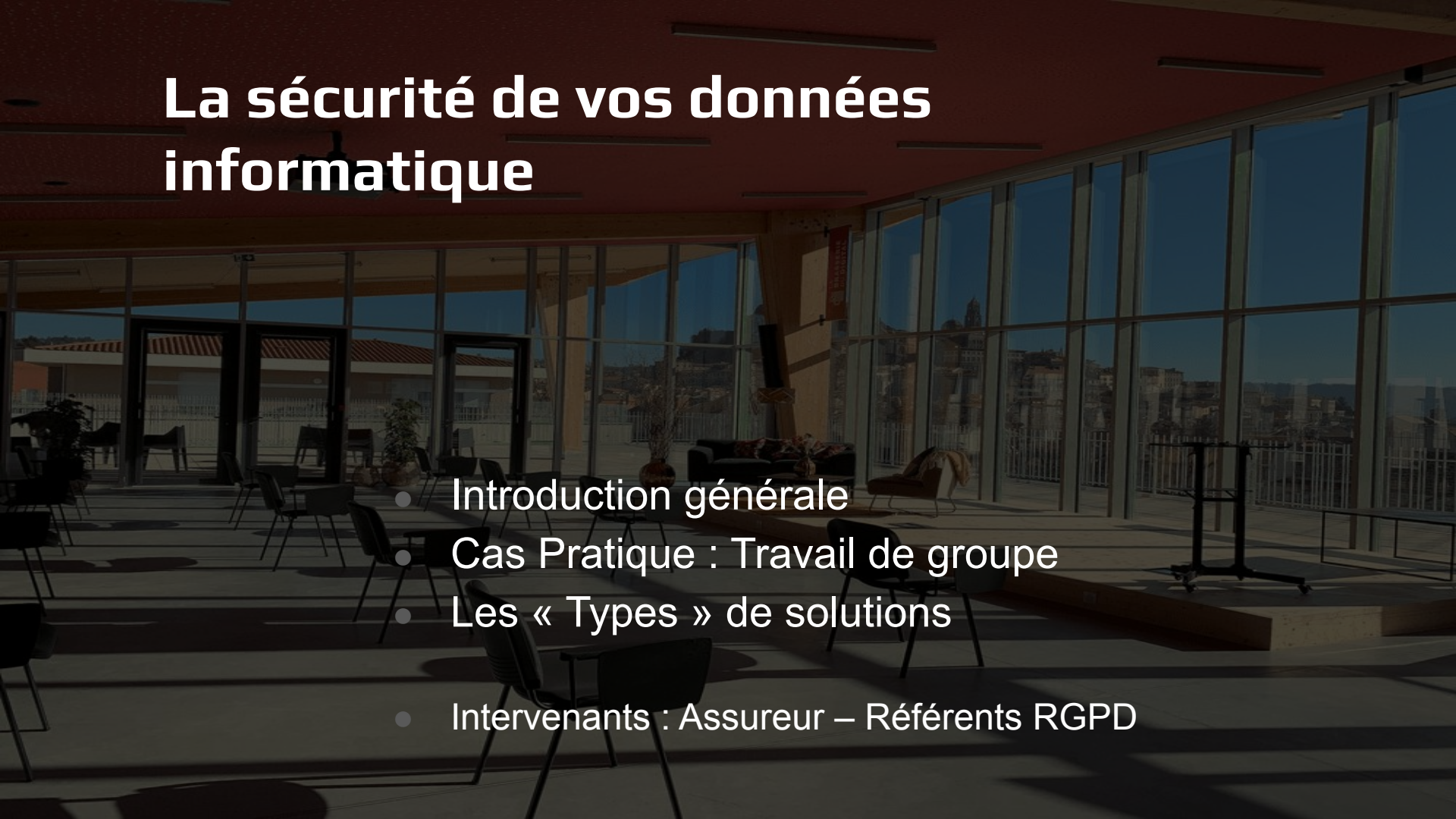
$79,841

33% dépensent plus pour résoudre le problème que ce qu'elles auraient dépensés pour le prévenir. [1]

(1) Source: Small Business Cyber Security Study, Microsoft & YouGov, April 2018

(2) Source: Better Business Bureau "2017 State of Cybersecurity Among Small Businesses in North America. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

La sécurité de vos données informatique



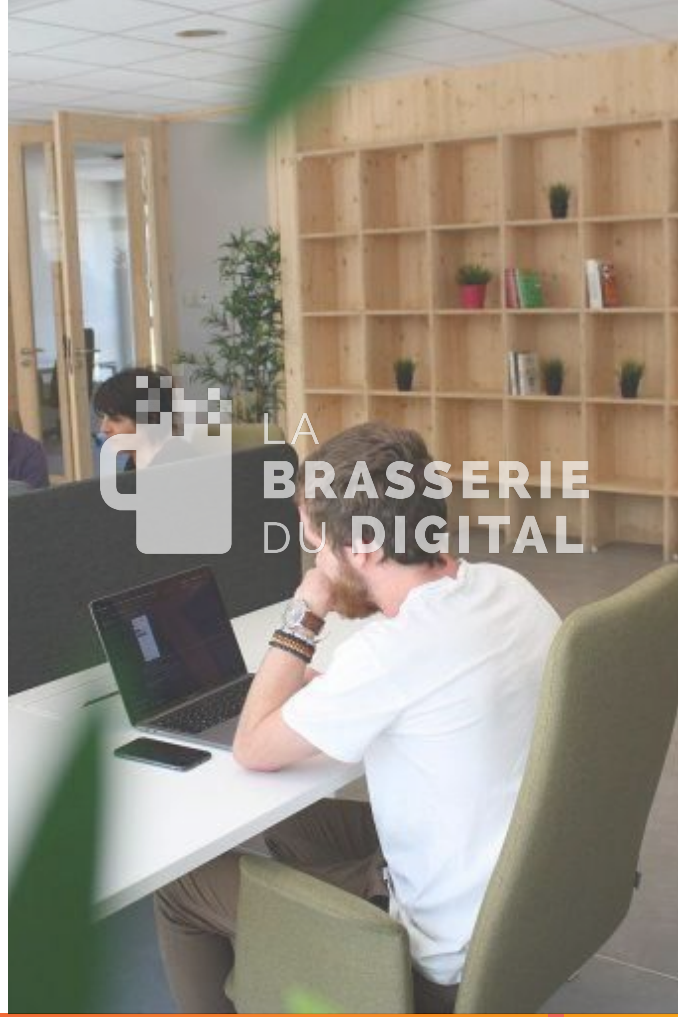
- Introduction générale
- Cas Pratique : Travail de groupe
- Les « Types » de solutions

- Intervenants : Assureur – Référents RGPD

Sécurité Informatique

Introduction générale

- Les Types de données
- Les failles de sécurité
- Les types d’attaques
- Les règles de sécurité



Exemples de données commerciales sensibles

"Prix que nous payons pour les produits"	"Prévisions de ventes"	**"Informations protégées sur la santé "**	"Informations de compensation"	**"Formulations de produits"**	**"Numéros de téléphone"**
"Carte de crédit et informations de permis de conduire qui nous sont envoyées par les clients"	*"Ingrédients qui entrent dans nos produits de soins capillaires"*	"Compte bancaire et numéros ABA"	*"Informations sur les passeports que nous recueillons auprès de nos 1099 sous-traitants internationaux"*	*"Demandes de crédit que les gens nous envoient"*	
"Finances d'entreprise "	"Fichiers d'employés que les RH conservent"	**“Listing des clients"**	**“…Et vous ?"**		

Les failles de sécurités

- L’authentification par mot de passe trop faible
- L’absence de règles d’authentification
- L’absence de chiffrage de données
- Les droits utilisateurs

59% Propagation de virus[1]

46% Attaque de ransomware[1]

34% Attaque d'hameçonnage[1]

27% Fuites de données[1]

(Les employés peuvent aussi être une source de risque)

Les clients PME ne sont pas équipés pour gérer eux-mêmes la sécurité informatique

- Manque d’expertise
- Pas assez de ressources
- Moins familier
- Submergé

Sécurité Informatique

Cas pratique : Et vous, dans votre entreprise…

- Les Types de données
- Les sécurités en place
- Gestion de crise :
  - Perte de données
  - Plan de reprise d’activité
  - Perte financière

Sécurité Informatique

Les types de solutions

- De la vision Technologique :
  - Les 5 leçons
- De la vision humaine :
  - RSSI
  - Juriste
  - Prestataire informatique
  - Assureur

5 Leçons

Recherche, approche et méthode

01 Prendre au sérieux la cybersécurité

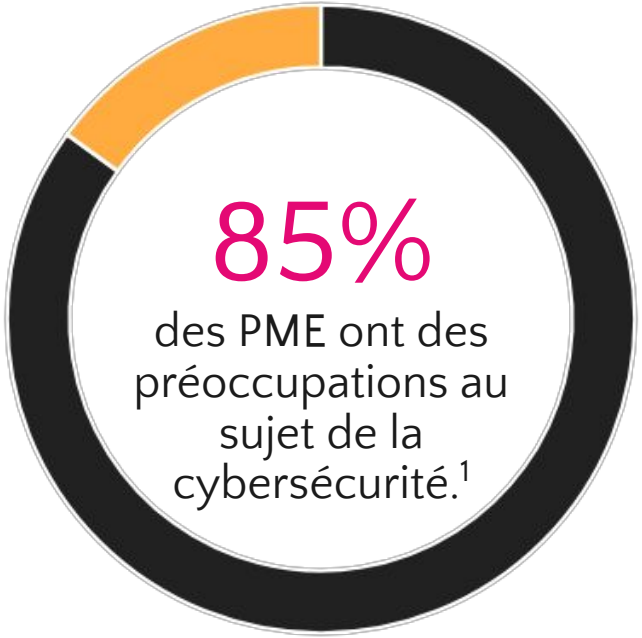
02 Il coute moins cher de prévenir plutôt que de guérir

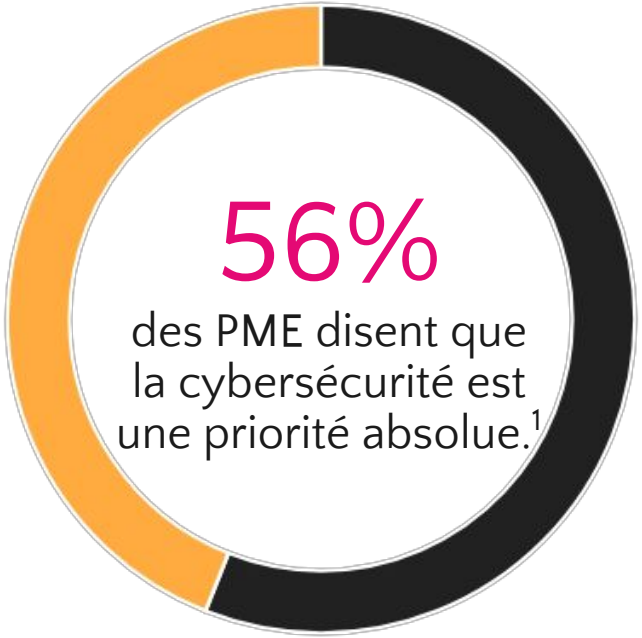
03 Faire plus avec moins

04 Focus sur les plus grosses menaces

05 Les failles existent: Quelle réponse apporter

#1 Prendre la cybersécurité au sérieux





Mais de nombreuses entreprises sous-estiment leur risque

Idée générale

74%

des entreprises ne croient pas qu'elles seront attaquées.[1]

2x

La plupart des PME croient que les grosses sociétés sont deux fois plus susceptibles d'être attaquées.[1]

Réalité

41%

des PME ont été attaquées au cours de la dernière année.[1]

Recommandations

Ne soyez pas complaisant

Apprenez les principes fondamentaux de la sécurité tels que les meilleures pratiques et les menaces les plus courantes

Etablir un ordre de priorités

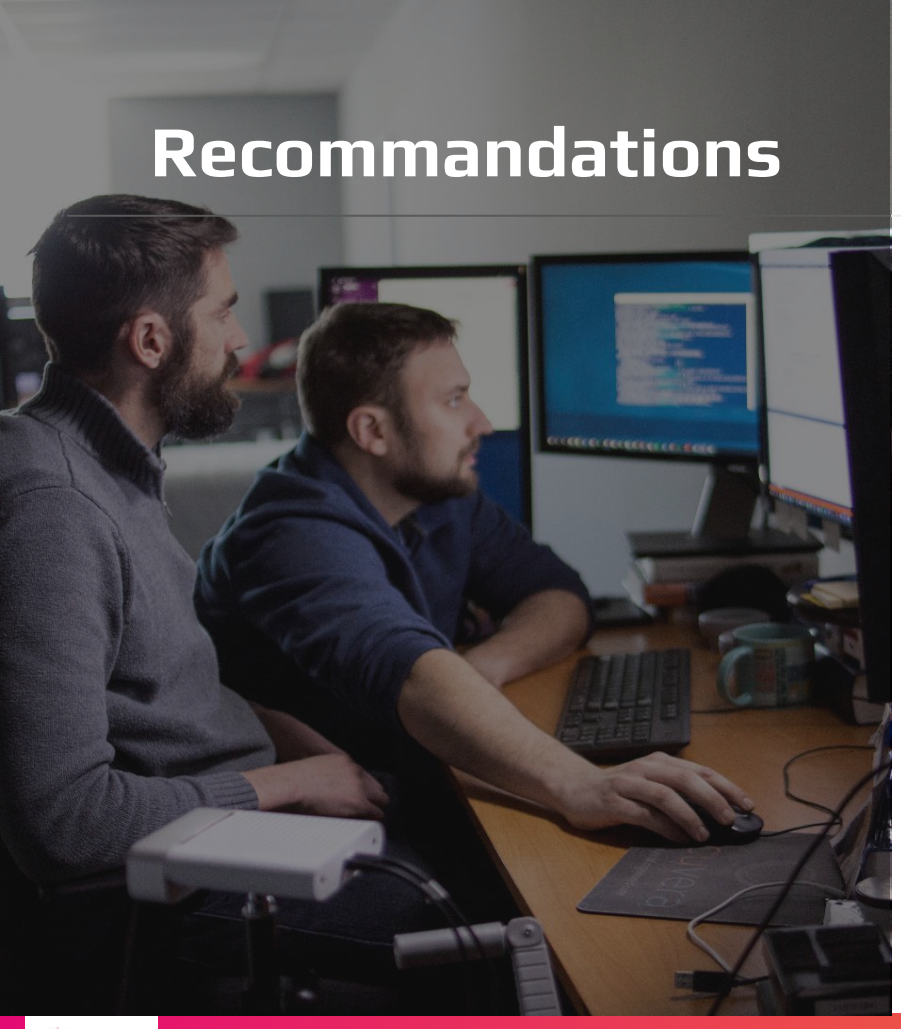
Réfléchissez à ce qui est le plus important pour votre entreprise

Protégez d'abord vos actifs prioritaires

#2 Il est moins coûteux de prévenir plutôt que de guérir

Les attaques sont chaotiques et désarmantes	Des protections adéquates réduisent la probabilité et la gravité des attaques
Des rôles de sécurité non définis peuvent augmenter les dégâts	Des rôles de sécurité définis permettent une action décisive qui limitera les dégâts
Les employés qui ont des habitudes risquées peuvent accroître la vulnérabilité	La formation des employés à la reconnaissance des menaces peut aider à atténuer les risques pour la sécurité

Recommandations



Adopter un état d'esprit soucieux de la sécurité

Définir et attribuer des responsabilités en matière de sécurité informatique

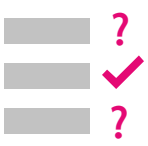
Avoir un budget dédié à la sécurité

Organiser une formation régulière des employés

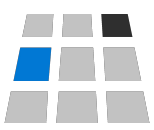
#3 Faire plus avec moins

Manque d'expertise
Pour rester vigilant face aux nouvelles menaces

Pas assez de ressources
Pour identifier, évaluer et atténuer les risques pour la sécurité

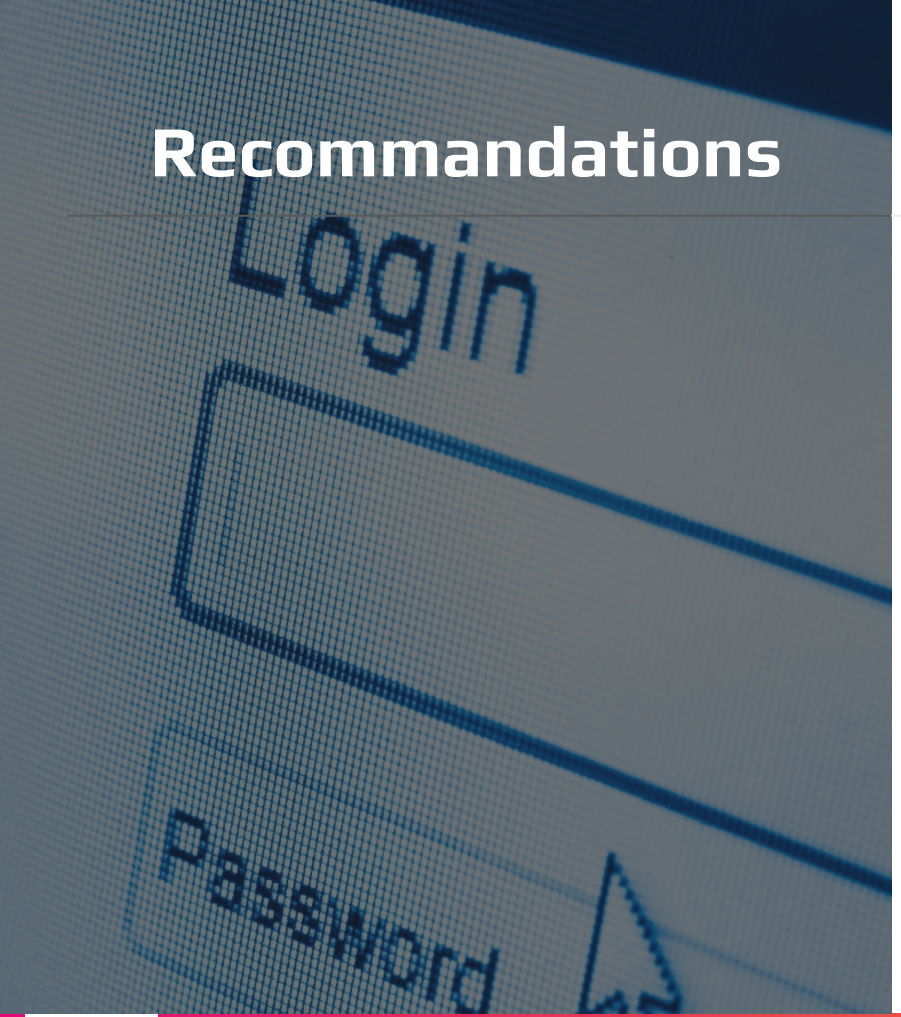


Moins familier avec les bonnes pratiques de sécurité



Submergé avec les offres de sécurité disponibles

Recommandations



Approche de sécurité pour les PME

- Appliquer un système d'authentification modern & fort
- Maintenir les systèmes à jour
- Modifier les noms d'utilisateur et mots de passe par défaut
- Examiner et utiliser les capacités de sécurité déjà à votre disposition
- Tirez parti d'un partenaire (vous) pour vous aider

#4 Se concentrer sur les plus grandes menaces

59%
Propagation de virus[1]

46%
Attaque de ransomware[1]

34%
Attaque d'hameçonnage[1]

27%
Fuites de données[1]

(Les employés peuvent aussi être une source de risque)

Propagation des virus

Installer un logiciel antivirus

Sécuriser les appareils de travail personnels et autres :

- Gestion des appareils mobiles
- Solution de gestion de l'identité et de l'accès
- Authentification multifacteur

60%

de violations proviennent de paramètres d'un appareil compromis comme un ordinateur portable ou un téléphone.[1]

Ransomware

Se défendre contre les attaques ransomware:

- Chiffrer et sauvegarder les données sensibles dans le cloud

En cas d'attaque :

- Embaucher un partenaire avec l'expérience ransomware

Hameçonnage (phishing)

Obtenez des outils dotés de capacités anti-hameçonnage

Informez les employés sur la façon de repérer et de signaler les courriels, les pièces jointes, les liens et les sites Web d'hameçonnage

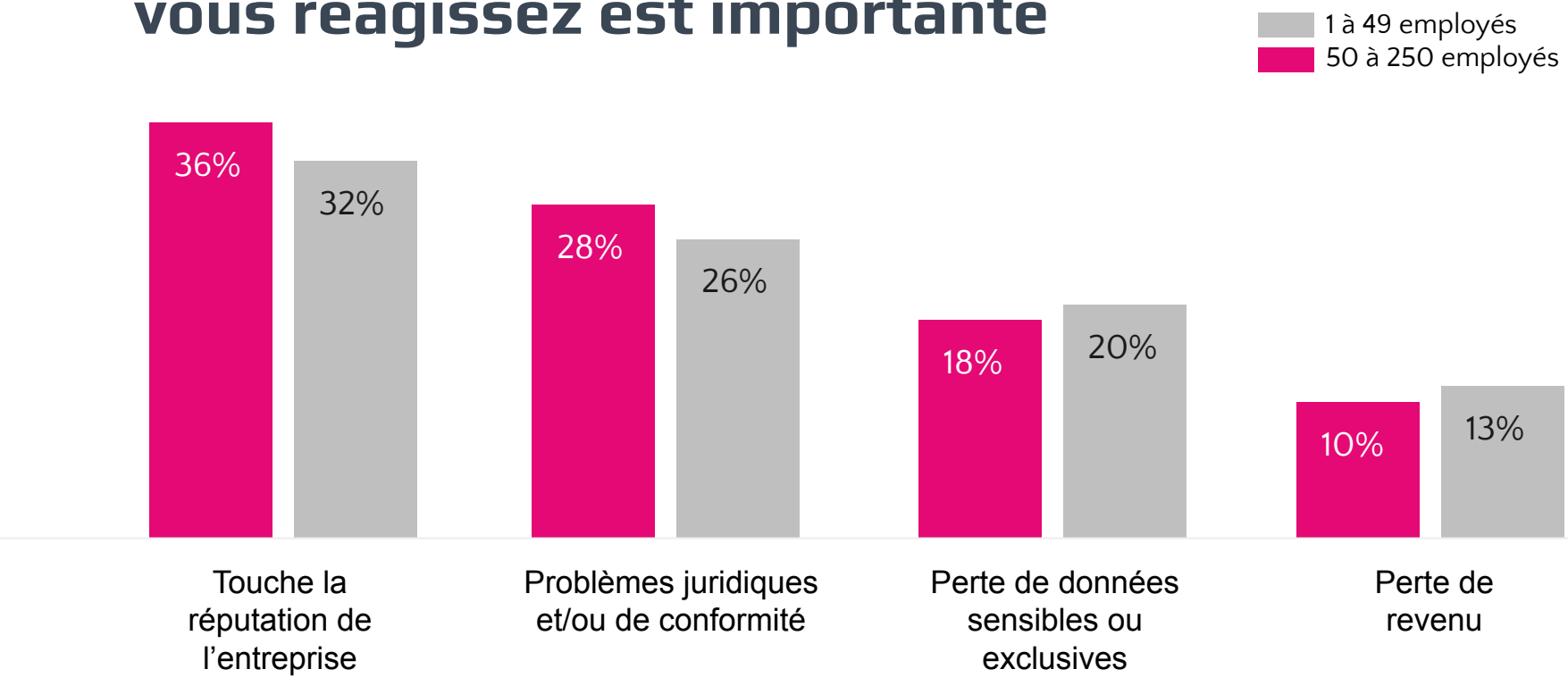
Fuites et partage de donn
sensibles par des employé

- Effectuer des examens périodiques de l'accès des utilisateurs aux données, aux appareils et aux réseaux
- Mettre en œuvre l'accès conditionnel
- Mettre en œuvre des solutions de protection de l'information :
  - Prévention des pertes de données
  - Protection au niveau des documents
  - Classification des données

53%

des entreprises ont été victimes d'attaques d'initiés contre leur organisation au cours des 12 derniers mois.[1]

#5 Des brèches existent : la façon dont vous réagissez est importante



Le temps de récupération fait des ravages

Avoir un plan pour réagir rapidement et efficacement

43%

des petites entreprises qui ont été attaquées a pris plus d'une semaine pour récupérer.[1]

80 000 $

coût moyen d'une attaque qui met plus d'une semaine à être résolue[2]

65%

des PME qui perdent l'accès à leurs données pendant plus de trois mois ferment.[3]

Conseils : développez votre entreprise en matière de sécurité

Les stratégies de sécurité les plus efficaces sont souvent les plus simples

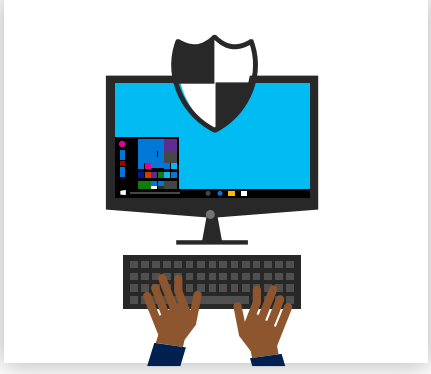
- Embauchez un partenaire ayant une expertise en matière de sécurité pour identifier et répondre à vos besoins particuliers en matière de sécurité
- Priorisez ce que vous devez protéger le plus
- Consacrez un budget pour mettre en place les bonnes solutions
- Ne soyez pas complaisant — développez une conscience de base des concepts et des risques de sécurité globaux

De la ressource humaine

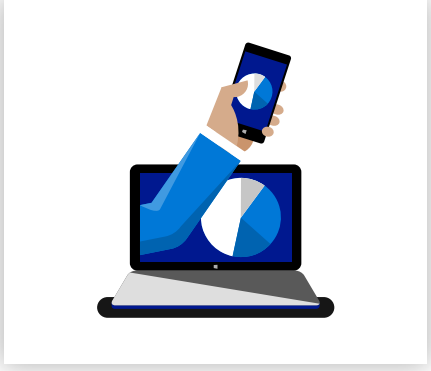
Faites vous entourer pour être mieux armé !

- RSSI
- Prestataire informatique
- Juriste
- Assureur

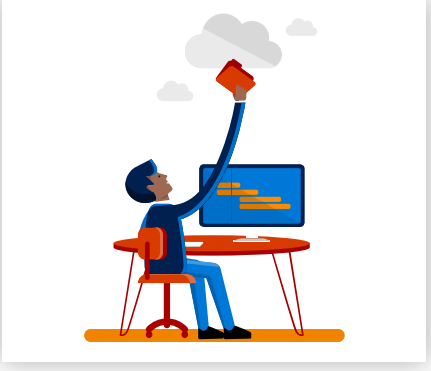
Le travail à distance commence par la sécurisation de l'identité et de l'accès



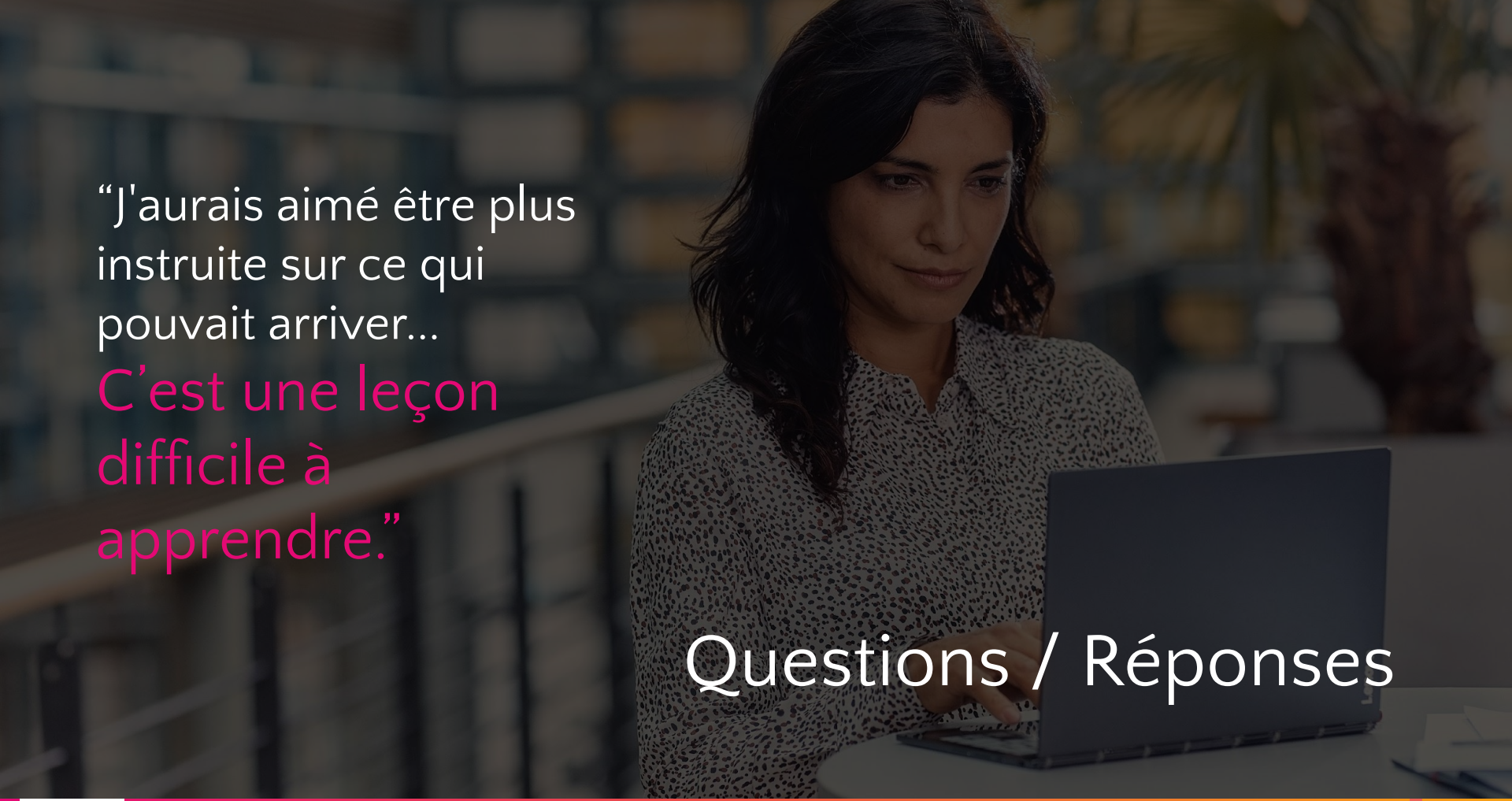
Protégez-vous contre les mots de passe perdus et volés



Accès sécurisé aux applications de travail



Gerez les rôles


“J'aurais aimé être plus instruite sur ce qui pouvait arriver...
C’est une leçon difficile à apprendre.”
Questions / Réponses

Merci pour votre attention !

LA BRASSERIE DU DIGITAL

Numérique du Pensio
4 rue du PNDF
43000 Le Puy-en-Velay

04 43 18 01 25
contact@labrasseriedudigital.com

www.labrasseriedudigital.com

B&C informatique

ZI de Bombes
Rue Maurice Shuman
43700 Saint Germain Laprade

04 71 03 54 22
laurent@bnc-informatique.fr

bnc-informatique.fr

strat &SI

23 rue de la République Saint-Etienne
Numérique du Pensio Le Puy-en-Velay

04 77 06 19 12
nicolas@strat-et-si.fr

strat-et-si.fr