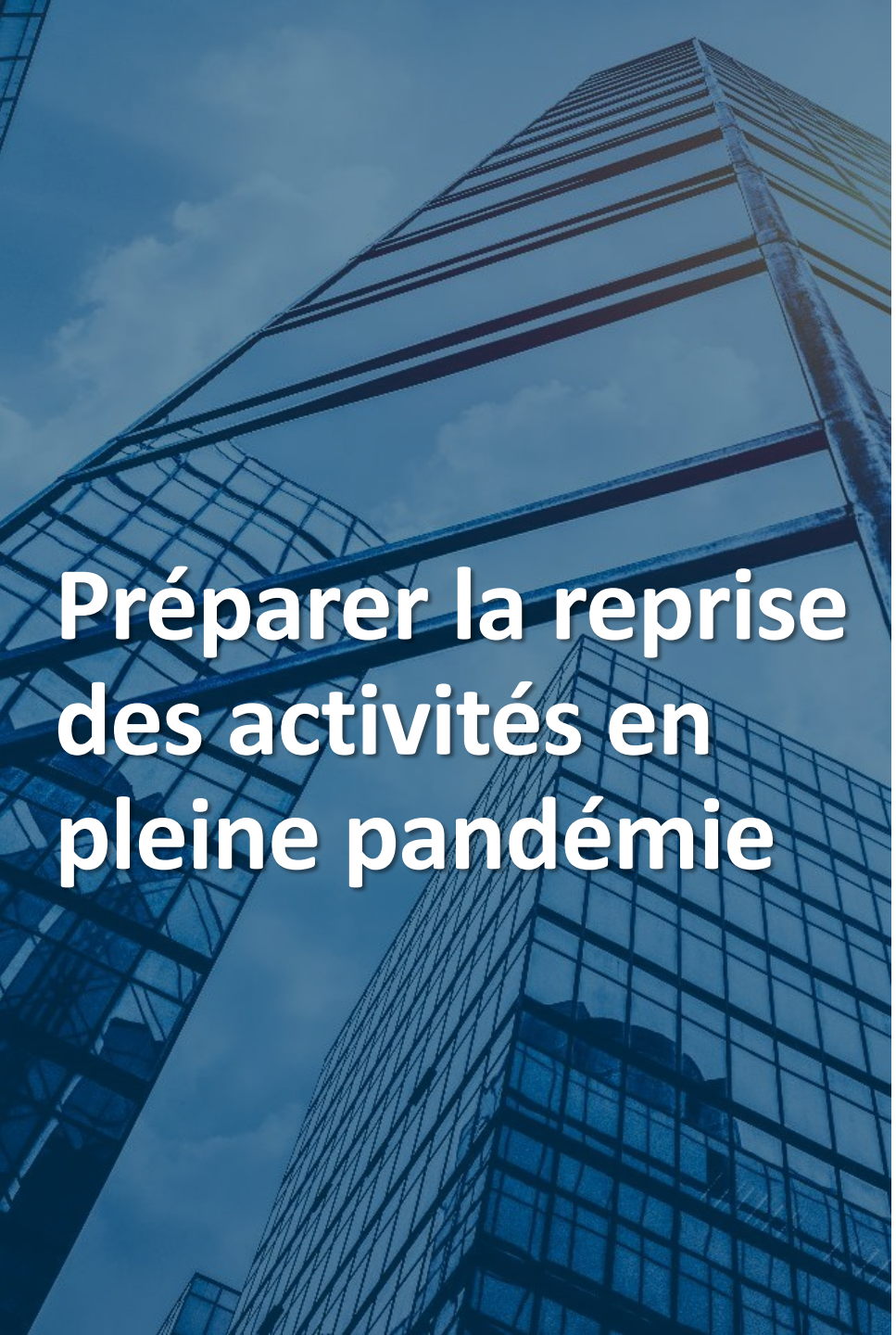
Guide SI de Reprise d'activité COVID-19

Après une longue période de confinement, il est temps d'organiser la reprise l'activité et le SI apparaît comme un outil pivot dans ce contexte de menace pandémique persistante et de retour progressif des ressources.

Tirer les enseignements de la crise coronavirus pour repenser la gestion des menaces et la transformation numérique.



Préparer la reprise des activités en pleine pandémie

Depuis fin 2019, l'épidémie de COVID-19 se propage rapidement à travers le monde, poussant les gouvernements à procéder à des confinements de masse dont **les impacts sont lourds et inédits sur les populations, les organisations et l'économie mondiale**. Parce que les organisations concourent au fonctionnement économique, à la production et la distribution de biens et de services indispensables, la relance de leurs activités est particulièrement nécessaire et attendue !

Durant la période de confinement liée à la crise sanitaire du COVID-19, **de nombreuses organisations (entreprises, collectivités, associations…) ont dû interrompre leur activité** ou au mieux la maintenir partiellement, en **recourant massivement au télétravail**, et souvent de façon arbitraire donc **sans stratégie de mise en œuvre** et de maintien en conditions. Dans le même temps et, comme redouté, **les activités cybercriminelles se sont intensifiées** pour profiter de cette situation de fragilité des organisations et de leurs collaborateurs.

EXTERN it.
conseil & expertises numériques

L'annonce du début du déconfinement le 11 Mai 2020, va permettre aux organisations de préparer une reprise progressive de leurs activités. Dans un premier temps, **le recours au télétravail reste toujours à privilégier** partout où c'est possible, les organisations doivent se préparer à cette reprise, tant sur le plan sanitaire que pour **reprendre le contrôle de leur système d'informations**, pour lesquels **la sécurité numérique**, les environnements de travail ont connu de brusques virages technologiques bien souvent inconnus et sur lesquels les organisations n'ont **pu bâtir une stratégie de mise en œuvre** et d'utilisation !

Ce guide a pour objet de vous orienter dans l'élaboration de votre feuille de route de reprise et de développement des activités notamment Informatiques.

D'une part, **l'impact lourd des confinements impose des chantiers de reprise des activités** et d'**ajustement organisationnel qui permettront le rebond à court terme**. Dans le même temps, il convient de s'adapter à un environnement désormais nouveau en menant des transformations en profondeur qui permettront la survie de l'organisation à long terme :

- Repositionnement stratégique,
- Renforcement de la sécurité des SI,
- Prise en compte des nouvelles menaces dans les plans de poursuite d'activité,
- Accélération de la transformation numérique en font partie.

ETABLIR UN PLAN D'ACTIONS CYBER

Les 10 mesures suivantes recommandées par les autorités cyber françaises visent à aider votre organisation dans la réalisation de leur plan d'actions cybersécurité de déconfinement.

EXTERN it.
conseil & expertises numériques

1 Recenser et analyser les incidents de sécurité

Les incidents de sécurité qui ont pu se produire durant le confinement doivent être recueillis, consignés et contrôlés pour s'assurer qu'ils n'ont pas engendrés de faiblesse dans la sécurité de l'organisation et pour les corriger au besoin.

Un appel à signalement complémentaire des collaborateurs pourra utilement être réalisé, avec des exemples concrets (exemples : hameçonnage de mot de passe, document suspect reçu en pièce-jointe d'un message…), pour cerner le plus précisément possible les incidents survenus.

2 S'assurer du bon fonctionnement de ses outils de protection

Il est primordial de s'assurer du bon fonctionnement des outils de sécurité avant d'envisager une reprise d'activité : antivirus, pare-feu, systèmes de détection d'intrusion…

Toute anomalie comme par exemple l'arrêt d'un antivirus sur un système critique, devra être considérée comme un signe possible d'attaque et investiguée comme telle.

3 Rechercher les indices de compromission

Les journaux des pare-feu, antivirus, proxy, serveurs critiques… doivent être analysés à la recherche de tout indice suggérant une possible cyberattaque comme des connexions inhabituelles, des détections de programmes malveillants ou des transferts anormaux d'informations.

Il conviendra également de vérifier les pare-feu à la recherche de nouvelles règles inappropriées, effecteur une revue des habilitations pour déceler toute création de nouveau compte suspect, ou présence de comptes inutiles ou clôturés. Ou encore les serveurs de messagerie pour repérer des règles de transferts de messages vers des comptes externes illégitimes, qui auraient pu être créées durant la période de crise.

4 Contrôler et tester les sauvegardes

L'actualité démontre que les sauvegardes sont déterminantes pour toute organisation victime d'une cyber-attaque.

Avant de reprendre l'activité de l'organisation, il est donc particulièrement important de vérifier leur bon fonctionnement, notamment en procédant à des tests de restauration et de s'assurer de disposer d'une copie récente des données qui soit déconnectée du réseau afin de pouvoir faire face à une attaque par rançongiciel.

5 Réaliser les mises à jour de sécurité en instance

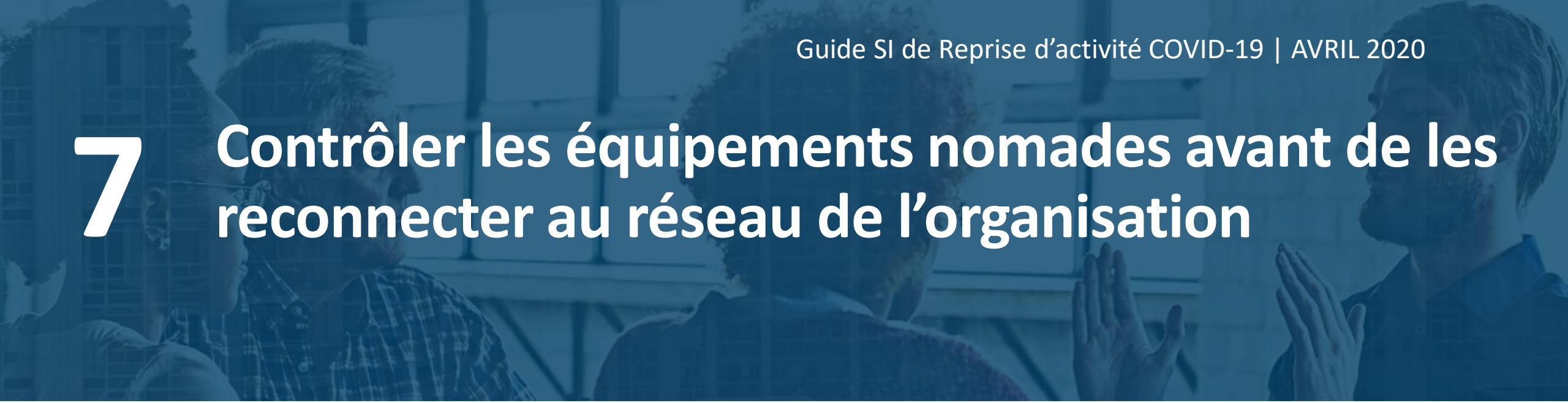
Si durant le confinement certains systèmes n'ont pas pu recevoir leurs mises à jour de sécurité, il convient de mettre en œuvre un plan de rattrapage cohérent et sans précipitation pour éviter tout effet de bord sur l'activité opérationnelle.

La priorité sera donnée aux systèmes de sécurité, puis aux systèmes ou serveurs critiques exposés directement ou indirectement sur Internet, et enfin aux postes de travail des collaborateurs.

6 Recentraliser les données

Durant le confinement, des données de l'organisation ont pu être dispersées sur les postes des télétravailleurs ou de manière temporaire sur certains services de d'hébergement externes (cloud).

Il convient donc de les recentraliser au sein de l'organisation pour s'assurer de leurs sauvegardes et de les supprimer dans les règles de l'art sur les stockages inappropriés pour limiter tout risque d'atteinte en matière de confidentialité.



7 Contrôler les équipements nomades avant de les reconnecter au réseau de l'organisation

Avant d'en ré-autoriser la connexion au système d'informations de l'organisation, tous les équipements nomades utilisés durant le confinement (ordinateurs portables, téléphones mobiles, tablettes) doivent faire l'objet d'un contrôle strict pour s'assurer qu'ils n'ont pas été compromis, et idéalement faire l'objet d'une réinstallation complète depuis une matrice maîtrisée, sécurisée et convenablement mise à jour par l'organisation.

8 Refermer les accès externes devenus inutiles

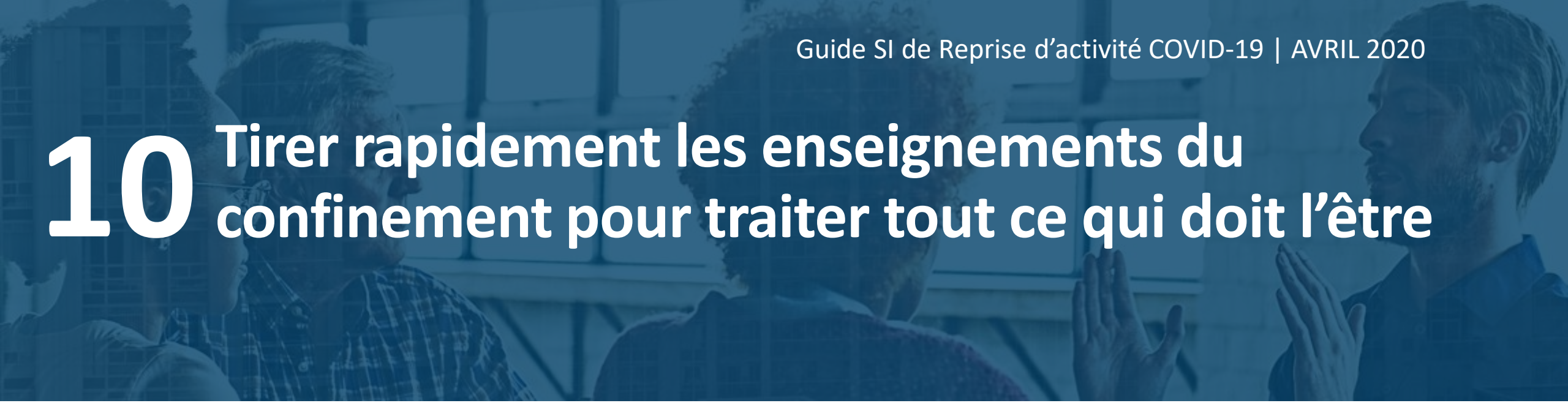
L'organisation doit s'attacher à réduire son exposition, et donc sa surface d'attaque, en refermant tous les accès externes ouverts qui seraient devenus inutiles.

Il peut s'agir d'accès externes à fermer au niveau des pares-feux mais aussi de comptes avec droits privilégiés ouverts à titre exceptionnel sur certains systèmes de l'organisation qu'il faudra clôturer.

9 Mettre fin aux usages à risques dérogatoires

Pour faire face au confinement, de nombreux usages d'applications, de services ou de pratiques ont pu être autorisés à titre exceptionnel mais peuvent présenter un risque de sécurité pour l'organisation.

Il convient donc de communiquer avec pédagogie et transparence sur l'arrêt d'autorisation de ces pratiques dérogatoires.



10 Tirer rapidement les enseignements du confinement pour traiter tout ce qui doit l'être

L'organisation doit savoir tirer les enseignements de la crise pour se préparer à avoir la capacité de mieux l'affronter en cas de résurgence.

Cela peut concerner sa politique d'équipement matériel en postes nomades professionnels maîtrisés pour les télétravailleurs, en équipements logiciels ou outils de travail à distance (visioconférence, téléconférence, hébergements de données…), en outils et procédures sécurisées de télétravail ou de téléadministration de ses systèmes, en infrastructures de sécurisation de ses systèmes, en formation et sensibilisation de ses collaborateurs, etc.

ETABLIR UN PLAN D'ACTIONS CYBER

- Recenser et analyser les incidents de sécurité
- S'assurer du bon fonctionnement des outils de protection
- Rechercher les indices de compromission
- Contrôler et tester les sauvegardes
- Réaliser les mises à jour de sécurité en instance
- Recentraliser les données
- Contrôler les équipements nomades
- Refermer les accès externes devenus inutiles
- Mettre fin aux usages à risques dérogatoires
- Tirer rapidement les enseignements du confinement

EXTERN it.
conseil & expertises numériques

DIGITALISER LE SI

Et les environnements de travail, afin de garantir la résilience et l'efficience du Système d'Informations

EXTERN it.
conseil & expertises numériques

1 Soutenir la numérisation des métiers

Des solutions organisationnelles et numériques ont été déployées dans l'urgence pour limiter les déplacements et pour éviter les contacts physiques. Le télétravail est le parfait exemple de solution informatique précieuse lorsqu'elle est bien mise en œuvre et acceptée par les utilisateurs.

Cette situation nouvelle porte préjudice aux organisations dont la maturité numérique est faible, à la faveur de leurs concurrents plus avancés.

On recommandera donc d'accélérer la transformation numérique de l'organisation dans une démarche projet. Contribuer à faire de la digitalisation des métiers et des échanges « un élément de différenciation » porteur d'avenir pour de nombreux secteurs, est un autre défi.

2 Sécuriser les évolutions numériques

Les usages numériques sont autant de nouveaux risques à prendre en compte. De plus, en période de télétravail généralisé, la cybercriminalité augmente fortement.

Il convient donc de renforcer la sécurité des systèmes d'informations :

- Analyser les risques informatiques et leurs éventuels impacts ;
- Évaluer le niveau de sécurité du SI et des données ;
- Définir des chantiers de renforcement de la cybersécurité adaptés aux transformations du SI ;
- Sensibiliser les utilisateurs.

3 Adapter les postes de travail

La crise a démontré qu'un grand nombre d'organisations n'ont pas encore adressé des sujets clés de développement, tels que la prise en compte de la mobilité ou encore les concepts de « Digital Workplace ».

Les services informatiques auront pour mission de favoriser l'adaptation et la flexibilité des outils de travail en permettant notamment le télétravail, en utilisant des équipements nomades (ordinateurs portables, smartphones, etc…) et des solutions de collaborations à distance (plateforme de travail d'équipe, solutions de visio-conférence, partage de documents, etc…).

Le défi majeur de cet enjeu sera d'intégrer la sécurité numérique comme besoin primaire lors de l'identification des solutions.

4 Adopter le Cloud dans le SI

Le cloud est, avec la cybersécurité, l'un des domaines d'après-crise les plus porteurs. L'équipe informatique doit renforcer son expertise du cloud hybride (public/privé) et du multicloud (plusieurs fournisseurs) pour optimiser ses investissements.

Les responsables IT devront aussi trouver l'équilibre entre les développements internes de solutions « maison » et l'achat de technologies tierces.

DIGITALISER LE SI

- Soutenir la numérisation des métiers
- Sécuriser les évolutions numériques
- Adapter les postes de travail
- Adopter le Cloud dans le SI

GOUVERNER LE SI

Face à ces nouveaux enjeux qu'imposent les crises mondiales

1 Piloter le travail à distance

Les départements IT se trouvent déjà dans l'obligation de concilier « travail à distance et agilité », avec méthode et en fonction des moyens dont ils disposent. L'enjeu d'avenir porte sur la conduite du changement et la capacité d'adaptation des utilisateurs métiers.

L'accès aux outils collaboratifs ne suffit pas, la formation et l'engagement des utilisateurs sont d'autres enjeux. L'équipe informatique doit être moteur et travailler main dans la main avec les Métiers, à défaut, elle se retrouverait dans l'ombre et subirait les choix de la Direction qui ne tiendront pas compte des contraintes techniques (sécurité, interconnexion d'applications, architecture, technologies maîtrisées par les compétences internes…).

2 Soutenir la cybersécurité

Qu'il soit partiel ou à temps plein, le télétravail, qui repose encore souvent sur des réseaux domestiques non sécurisés, expose davantage les systèmes d'informations des organisations aux risques cyber.

L'équipe informatique devra renforcer la sécurisation des accès aux ressources de l'organisation quel que soit le lieu de connexion des équipes. La gestion des identités et des accès (IAM) fait donc partie des priorités, tout comme l'authentification multi-facteurs et la protection de données (traçabilité, cryptage…).

3 Sélectionner les partenaires IT

La résilience des fournisseurs de prestations externes devrait aussi faire l'objet d'une attention renforcée des responsables informatiques. Il s'agit, entre autres, de distinguer les fournisseurs de prestations critiques pour les intégrer dans une approche de travail/pilotage à distance.

Il est aussi temps d'intégrer à votre organisation des compétences à forte valeur ajoutée, en temps partagé, pour accompagner la croissance de l'entreprise.

4 Effectuer une analyse de risques numériques

À la lumière de la crise du Covid-19, les organisations devront effectuer des mises à niveau complètes et périodiques de leur cartographie des risques. Au-delà de la pandémie, elles devront désormais prendre en compte l'apparition de nouvelles menaces plus systémiques, parfois invisibles, à dimension internationale, voire récurrentes. Parmi celles-ci :

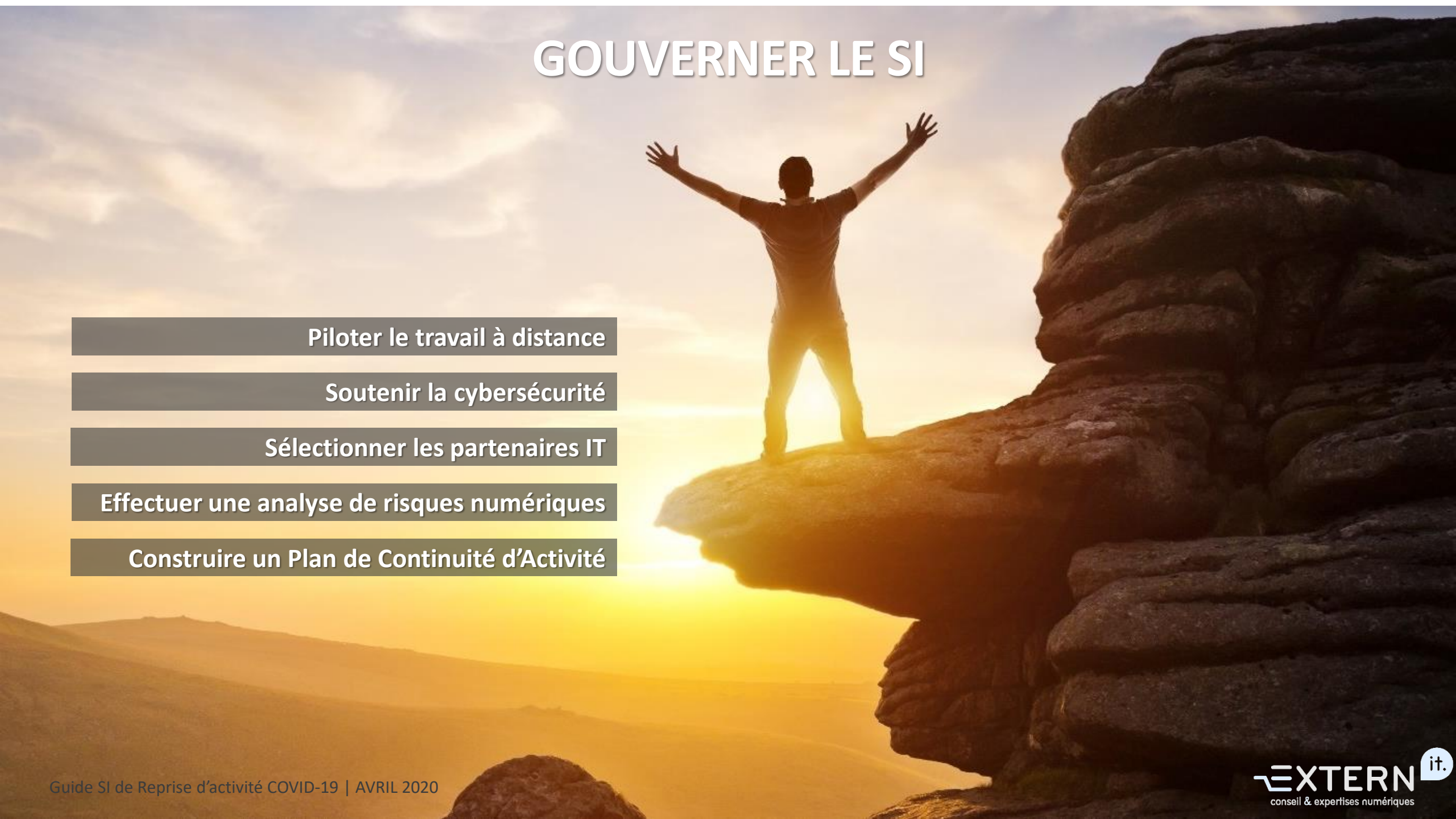
- Les nouvelles formes du terrorisme ;
- Les nouveaux mouvements sociaux ;
- Les évènements climatiques et sanitaires ;
- Les cyberattaques.

5 Construire un Plan de Continuité d'Activité

Prévoir la survie de l'organisation en crise. La continuité d'activité est un processus clé de l'organisation qui vise à assurer le fonctionnement en mode dégradé d'une organisation en cas de sinistre majeur. Elle se concrétise par la mise en œuvre d'un PCA: «plan d'urgence et de poursuite d'activité».
La gestion de crise est au cœur de ce dispositif. Pour être efficace dans l'urgence, il est indispensable d'avoir au préalable :

- Déterminé les processus clés ;
- Identifié les scénarios de risques ;
- Mis en place et partagé des solutions organisationnelles et techniques activables en cas de crise.

GOUVERNER LE SI



- Piloter le travail à distance
- Soutenir la cybersécurité
- Sélectionner les partenaires IT
- Effectuer une analyse de risques numériques
- Construire un Plan de Continuité d'Activité

EXTERN it.
conseil & expertises numériques

Pour nous contacter

www.extern-it.fr

contact@extern-it.fr

03.74.09.58.39

EXTERN it.
conseil & expertises numériques

NOS OFFRES SPÉCIALISÉES

- **Audit & Conseil Informatique**
  Lien web
- **Pilotage et Gestion SI**
  Lien web
- **Transformation Numérique**
  Lien web

EXTERN it.
conseil & expertises numériques

En savoir plus sur EXTERN it.

conseil & expertises numériques

Extern IT est une société de conseil en management de systèmes d'informations créée en 2017, rayonnant en régions Hauts de France et Île de France. Notre organisation travaille dans de nombreux secteurs d'activités. Notre équipe est composée de talents en informatique certifiés sur de nombreuses technologies et méthodes de pilotage SI.