Etude sur la gestion de crise et la résilience des SI

Quels impacts et nouveaux enjeux liés au Covid-19 ?

Décembre 2020

pwc

Sommaire

L'enquête a été menée entre juillet et septembre 2020 auprès d'un large panel d'entreprises en France et a visé les fonctions de management, de gestion des risques et continuité ou la sphère des professionnels des systèmes d'information.

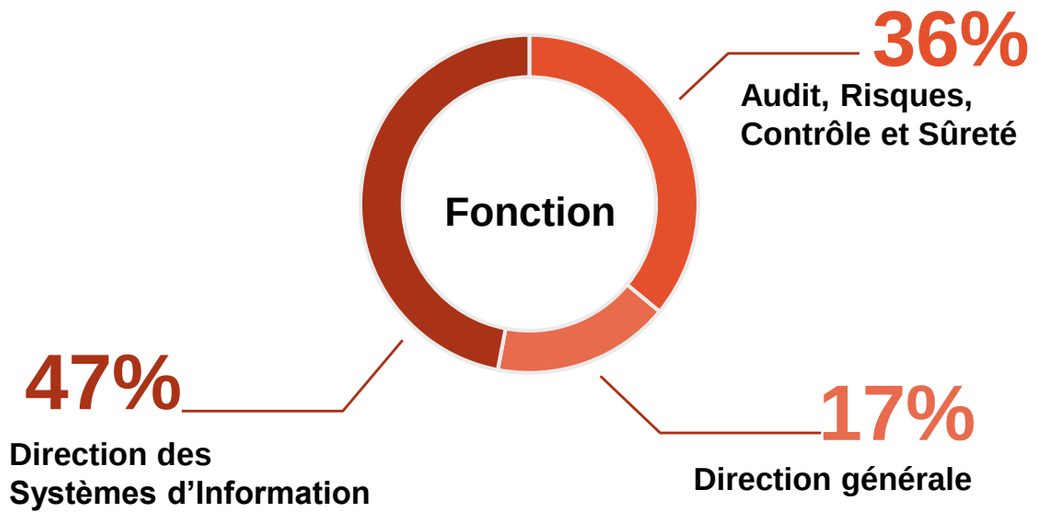
L'objectif de cette étude est de dresser un panorama sur la façon dont les organisations, quelle que soit leur taille ou secteur d'activité, ont fait face à la crise inédite du Covid-19. Un focus a été plus particulièrement réalisé sur les impacts subis au début de la crise ainsi que durant le premier confinement.

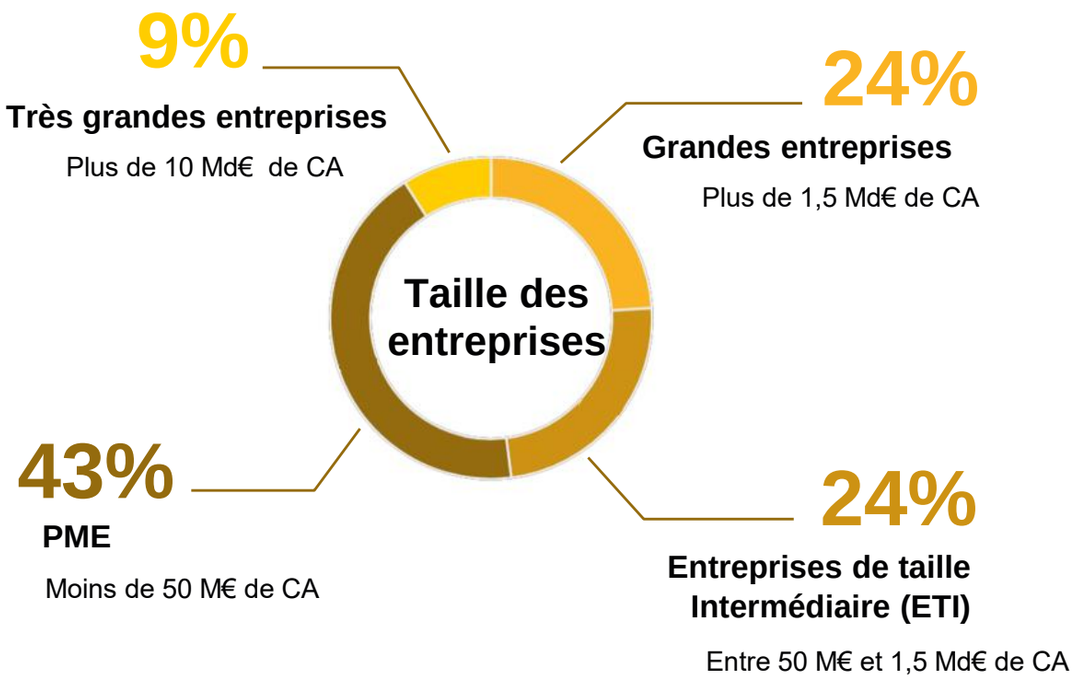
Les résultats permettent d'apporter un éclairage sur la perception de la gestion de la crise Covid-19 en termes de résilience des SI.

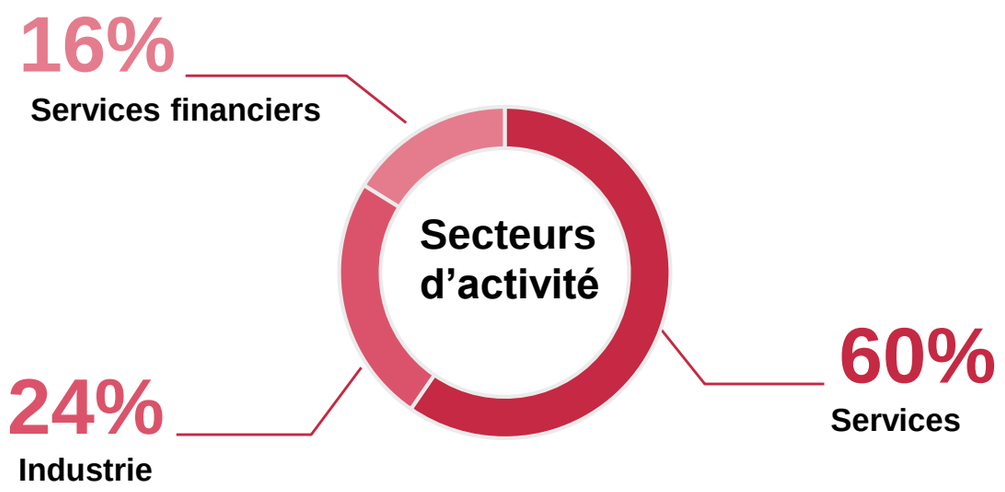
Profils des répondants

Présentation des profils des répondants à l'enquête concernant la gestion de crise et la résilience des systèmes d'information.

Enquête réalisée entre Juillet et Septembre 2020







Les points clés de l’enquête

La crise du Covid-19 et le confinement sanitaire imposé par les états durant la fin de l’hiver et le printemps 2020 ont forcé les entreprises à s'adapter rapidement au travail à distance mais également à définir et mettre en place les mesures nécessaires pour permettre massivement une telle agilité. Cette étude revient sur cet évènement et ses conséquences sur la résilience des systèmes d’information et la gestion de crise.

1 Lors du passage au travail à distance, près de **8 personnes sur 10** ayant répondu à l’étude **ont rencontré des difficultés** à différentes échelles.

2 D’un point de vue organisationnel, les principales perturbations relevées sont dues **à l’inadéquation des plans de gestion de crise et de continuité d’activité, et/ou un manque de préparation et de formation.**

3 Du point de vue des solutions, les difficultés sont liées d’abord à **l’absence de solutions logicielles** sur lesquelles s'appuyer, ainsi qu’au **manque de matériel physique (PC)** en quantités suffisantes pour doter l’ensemble des collaborateurs d’outils de télétravail.

4 Les **principaux incidents** rencontrés sont liés à **la capacité et la performance des infrastructures** disponibles.

5 Au niveau de **la sécurité**, **1/4 des répondants** a estimé que son entité avait dû faire des choix pouvant compromettre la sécurité des systèmes d'information de l’entreprise, principalement liés à **l’utilisation de solutions logicielles dont l’assurance en termes de confidentialité pouvait être mise en doute**.

6 Cependant, cela ne s’est pas traduit pour autant par une augmentation significative du nombre d’incidents de sécurité au cours de la période.

Pour **2/3 des dirigeants** interrogés, **le manque de résilience de l’infrastructure** dans le cadre du télétravail massif a été perçue comme **un facteur limitant.**

7 Enfin, pour **86% des répondants**, la crise a **renforcé les enjeux de résilience**, tant d’un point de vue opérationnel, que pour la dimension liée aux systèmes d'information.

Face au contexte de crise et d’incertitude, la **résilience des systèmes d’information** est devenue un nouvel **enjeu majeur** des entreprises.

Résultats de l’enquête

Travail à distance, difficultés rencontrées et points de blocage

78% des interrogés ont rencontré des **difficultés** principalement temporaires liées aux systèmes d'information lors du passage en télétravail

52% des dispositifs de réponse ont été **jugés inadaptés** durant la crise Covid-19.

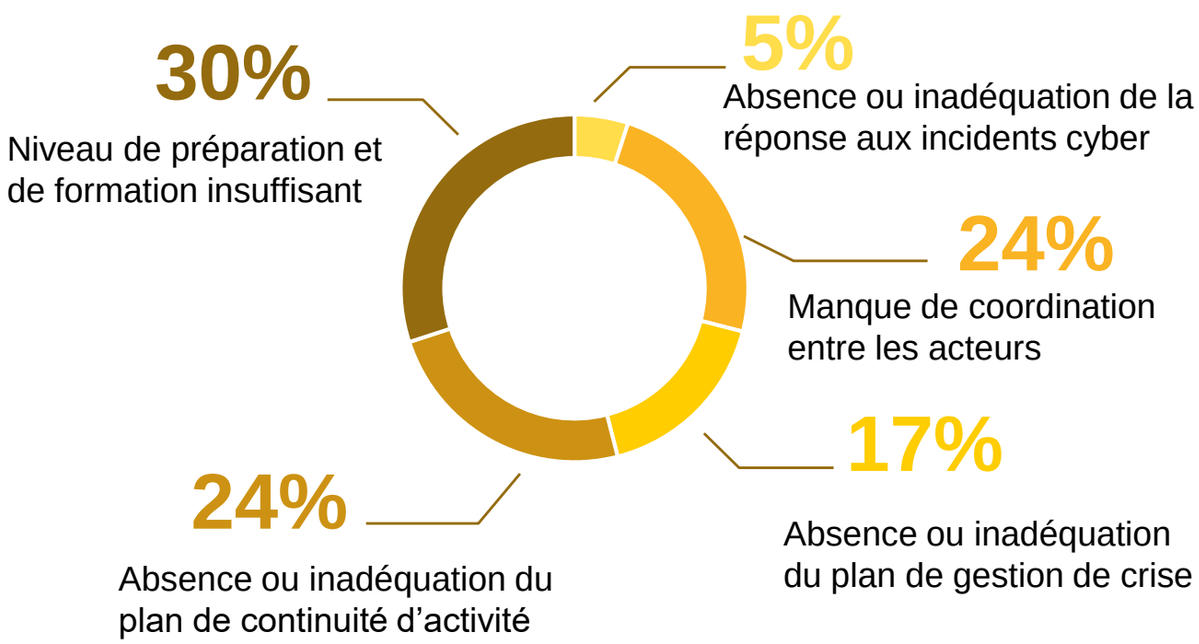
Parmi les personnes interrogées, **près d'une personne sur dix a rencontré des difficultés majeures** (incapacité d'accès durable au SI, infrastructure sous-dimensionnée…) principalement sur un volet bureautique.

Pour la très grande majorité des répondants, ceux-ci ont cependant connu des perturbations mineures ou temporaires.

Ainsi, pour la majorité des entreprises, la bascule vers le télétravail n'a pas été ressentie comme une épreuve majeure.

Cependant, les répondants ont constaté que les dispositifs en place n'étaient pas adaptés, une telle situation n'ayant pas été envisagée dans les scénarios de gestion de crise et de continuité d'activité.

Points de blocage rencontrés durant la crise de la Covid-19



Impact principal de la crise sur les systèmes d’information

35% **des infrastructures IT n'étaient pas adaptées à l'usage du télétravail massif.**

Impacts sur les outils informatiques

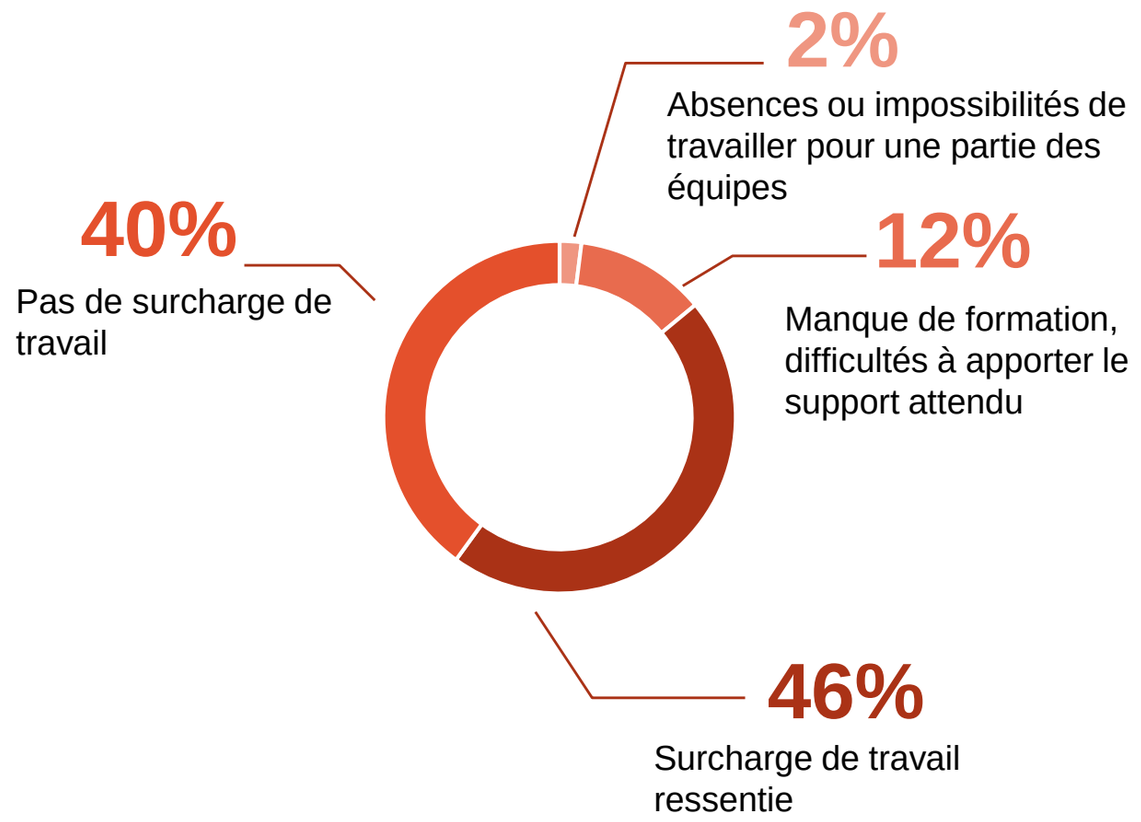
Les infrastructures n'étaient pas adaptées à l'usage du télétravail massif et n’ont pas pu supporter la charge engendrée par l'afflux de connexions distantes.

46% des interrogés ont déclaré que leur entreprise n’avait pas à disposition les logiciels nécessaires pour réaliser un travail à distance en sécurité (VPN, outils bureautiques, cloud, bureau virtuel, etc.).

38% des entreprises ont dû faire face à une insuffisance d'infrastructures physiques. Les répondants ont souligné le manque de disponibilité de postes de travail pour tous les employés.

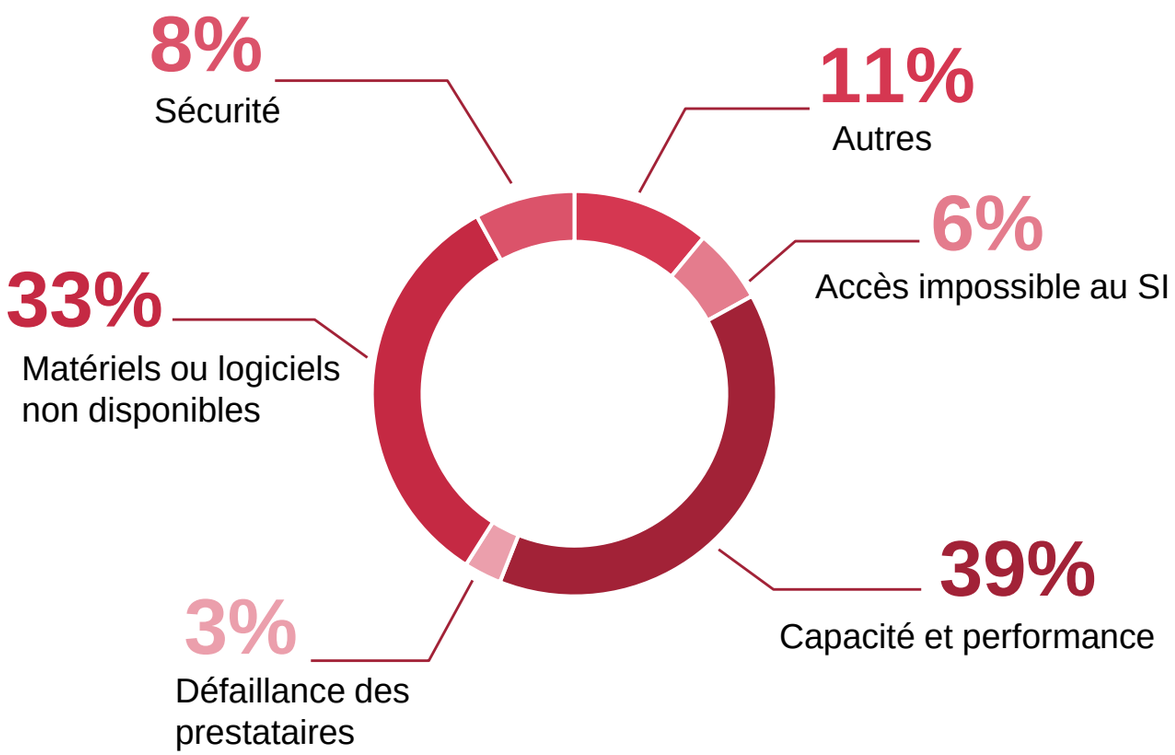
Enfin pour **2/3 des dirigeants, le manque de résilience** de **l’infrastructure** a été perçue comme un **facteur limitant**.

Impacts sur les équipes informatiques



Incidents et gestion de la sécurité des systèmes d'information

Typologie des incidents rencontrés pendant la crise COVID-19



1/4 **des entreprises a dû réaliser des arbitrages sur sa sécurité** pour poursuivre son activité.

Top 3 des compromis de sécurité

#1 **Confidentialité dans le mode d'échange des données** (Zoom, outil de partage de documents dans le cloud public)

#2 Sécurité physique des équipes IT

#3 Gestion des licences

Malgré les compromis en matière de sécurité, il n'y a pas eu de recrudescence d'incidents de sécurité.

Les principales **causes d'incidents sont liées à des sujets de résilience** (capacité et performance des systèmes d'information et manque de matériel adéquat) et non pas à cause de la cyber-résilience.

La résilience des SI et nouvelles priorités

20% **des entreprises interrogées estiment avoir eu un dispositif de résilience satisfaisant** pour affronter la crise de manière sereine.

Les déficiences du dispositif de résilience ont principalement été relevées par les équipes d'audit, de contrôle interne ainsi que par les directions des systèmes d'information.

86% **des répondants ont confirmé que la crise a renforcé l'enjeu de la résilience,** tant d'un point de vue opérationnel que dans sa dimension des systèmes d'information.

Top 3 des actions prioritaires remontées par les entreprises

1. Revoir le dispositif de gestion de crise et de continuité d'activité
2. Mener un audit / retour d'expérience sur la résilience du système d'information
3. Revoir le dispositif de continuité du système d'information

Face au contexte de crise et d'incertitude, la **résilience des systèmes d'information** est devenue un nouvel **enjeu majeur** pour les entreprises.

Quelles bonnes pratiques envisager pour renforcer la gestion de crise et la résilience de votre SI ?

- Faire évaluer la maturité du dispositif dans sa globalité pour disposer d'un confort suffisant en cas de perturbations ou incidents d'exploitation, sinistres ou risques cyber.
- Faire émerger les points forts et faiblesses afin de disposer d'un plan d'actions de renforcement des dispositifs, gestion de crise et de résilience du SI.
- Identifier les scénarios de crises nécessitant la mise en place de mesures de détection et de réponse dans le cadre du dispositif de gestion de crise.
- Identifier et classer les applications, services ou infrastructures critiques en fonction des activités de l'organisation (en intégrant la dimension externalisée).
- Mesurer l'impact sur la dimension métier en cas de 'perte' de l'actif ou du service au regard des risques encourus.
- Développer et évaluer les dispositifs et moyens de réponse disponibles garantissant en amont la résilience sur les volets :
    - Technique (architecture du SI…)
    - Processus opérationnels (gestion des incidents…)
    - Humain (hommes clés, GPEC…)

  en interne et au niveau de l'écosystème partenaires.
- Mettre en place ou actualiser le dispositif de gestion de crise pour une coordination d'ensemble.
- Adapter le plan de continuité métier et IT face aux nouveaux scénarios à envisager.
- Réaliser des tests et des exercices pour entraîner et s'assurer de l'opérationnalité des dispositifs.

Vos contacts PwC

Jean De Laforcade
Associé Risques Technologiques
Risk Assurance & Advisory Services

Bureau : 01 56 57 64 19
Mobile : 06 69 66 12 62
jean.de.laforcade@pwc.com

Thierry Delville
Associé
Sécurité globale

Bureau : 01 56 57 41 56
Mobile : 06 71 57 90 15
thierry.delville@pwc.com