FUTURE OF FINANCE

RÉSILIENCE DE LA TRÉSORERIE : BÂTIR UN PLAN D'ACTION EFFICACE

Astran

LOSAM

SOMMAIRE

SOMMAIRE

EDITO

Quand la trésorerie s'arrête, tout s'arrête. Les engagements financiers essentiels ne sont plus honorés : paiement des salaires, règlement des fournisseurs critiques, service de la dette et flux de trésorerie du groupe.

Une telle situation est intenable. Pourtant, des entreprises majeures telles que Marks & Spencer ou Jaguar Land Rover l'ont vécu récemment.

La dépendance croissante aux systèmes d'information expose aujourd'hui les directions financières à un risque systémique. **En cas de cyberattaque majeure ou de défaillance d'un fournisseur critique, la fonction trésorerie peut ne plus être en mesure d'assurer ses missions vitales.** Dans ce contexte, identifier les paiements prioritaires, exécuter les paiements de manière fiable et vérifier les coordonnées bancaires deviennent des défis opérationnels immédiats.

Cette perte de maîtrise peut conduire à une paralysie totale de l'organisation, générant des impacts financiers majeurs et une érosion rapide de la confiance des partenaires, des salariés et des marchés.

C'est pour cette raison qu'une quinzaine de directeurs de trésorerie de grands groupes français s'est réunie dans le cadre de la **Taskforce Treasury Resilience and Efficiency.** Leur objectif commun : **établir un plan d'action efficace permettant d'assurer la résilience de la trésorerie.**

Pour ce faire, ils ont travaillé ensemble sur quelques questions clés :

Quels processus métiers critiques ne doivent jamais s'arrêter (paiement des salaires, dettes, fournisseurs stratégiques) ?

Comment s'assurer que les données vitales restent disponibles lorsque les outils habituels, y compris les outils cloud, ne sont plus accessibles ?

Quelles relations bancaires privilégier en cas de crise : multi banques vs banque unique et stratégique dédiée à certains process ?

Comment construire un Business Case solide pour convaincre le Comex d'investir dans la résilience de la trésorerie ?

Quels sont les alliés stratégiques à embarquer (cyber, achats, banques, contrôle interne) et comment les convaincre ?

Comment utiliser un Digital Resilience Business Case (DRBC) comme base commune entre trésorier, CFO et partenaires externes ?

Si ce rapport ne peut répondre de manière personnalisée à chaque contexte, l'ambition du groupe de travail a été de proposer des recommandations claires et accessibles. **Elles doivent permettre à chacun de définir un plan d'action adapté, garantissant que les processus vitaux de trésorerie ne soient jamais interrompus.**

Yosra JARRAYA
ASTRAN
CEO et Co-founder
yosra.jarraya@astran.ai

WORKSHOP #1

RÉSILIENCE DE LA TRÉSORERIE DU BUSINESS CASE AUX ALLIANCES STRATÉGIQUES

Les travaux de la Taskforce mettent en évidence la nécessité de renforcer la prise de conscience des risques cyber pesant sur la trésorerie.

La résilience de la trésorerie ne peut donc être traitée comme un sujet strictement financier : elle suppose de mobiliser, dès l'amont, l'ensemble des acteurs clés, dont la composition peut varier selon les organisations (finance, IT, cybersécurité, opérations, achats).

Dans la majorité des entreprises participantes, le membre du comité exécutif en capacité d'**arbitrer et d'engager une stratégie de résilience** de la trésorerie est le Directeur Financier (CFO), et dans certains cas le Directeur des Opérations (COO). Sa décision s'appuie sur l'expertise métier de la Direction Trésorerie, en étroite collaboration avec la Direction Cyber, en charge de la résilience globale. Le CFO (ou le COO) arbitre également la répartition budgétaire, selon les politiques internes : certains coûts pouvant être portés par l'IT ou la cyber (licences, solutions), tandis que la mise en œuvre et le support relèvent selon les cas de la finance, des opérations ou de la cyber.

Afin d'éviter la dispersion et de maintenir un budget maîtrisé, la Taskforce recommande une approche pragmatique consistant à ne **protéger que les processus vitaux de l'entreprise**, sans chercher à répliquer l'ensemble du système d'information. Cette logique, qualifiée de Minimum Viable Company (MVC), repose sur une analyse simple : mesurer l'impact qu'aurait une crise cyber majeure – dont la durée moyenne est estimée à 21 jours selon Gartner – sur chaque processus. Cette méthode permet de construire un business case efficace, fondé non sur un ROI théorique mais sur les conséquences opérationnelles concrètes d'une paralysie de la trésorerie.

Les participants se sont accordés sur trois processus vitaux relevant de la Direction Trésorerie : **le paiement des salaires, le paiement des fournisseurs critiques et les processus de « pure trésorerie »** (tels que le service de la dette, le règlement-livraison des opérations de marché ou les flux intragroupe). Pour environ un tiers des entreprises, le processus de facturation clients est également considéré comme critique.

Enfin, les travaux soulignent que la résilience de la trésorerie constitue aussi un levier de transformation. La cartographie des processus, des flux et des systèmes permet non seulement de sécuriser l'existant, mais aussi de simplifier l'organisation, d'identifier les données réellement critiques et de renforcer la gouvernance. À ce titre, **la protection de la trésorerie doit être portée et arbitrée au niveau du comité exécutif, comme une décision stratégique de continuité et de maîtrise du risque, et non comme un simple projet technique.**

MOBILISATION EN INTERNE
QUAND LA PROTECTION DE LA TRÉSORERIE EST UN OUTIL DE TRANSFORMATION

MESURER L'IMPACT D'UNE CRISE SUR LA TRÉSORERIE

Les attaques par ransomware génèrent des interruptions d'activité prolongées et des impacts financiers considérables, comme l'illustrent deux incidents majeurs en 2025 : Jaguar Land Rover (cyber attaque) et Marks & Spencers (ransomware).

DURÉE D'ARRÊT

JAGUAR LAND ROVER	MARKS & SPENCERS
± 6 semaines	**± 46 jours**

COÛTS DIRECTS

JAGUAR LAND ROVER	MARKS & SPENCERS
196M£	**300M£**

IMPACT FINANCIER

JAGUAR LAND ROVER	MARKS & SPENCERS
11% du bénéfice 2024/2025	**30% de la marge (1/3 du bénéfice prévisionnel)**

IMPACT SYSTÉMIQUE

JAGUAR LAND ROVER	MARKS & SPENCERS
Facilité de crédit garantie État : 2Md£, -0.1% PIB UK (T3 2025)	**Impact sur les marges et l'EBITDA**

Ces incidents illustrent comment un seul événement cyber peut affecter significativement la performance financière et opérationnelle de grands groupes, avec des répercussions dépassant le périmètre de l'entreprise.

Contexte sectoriel : durée moyenne d'arrêt 21-24 jours (Statista, Coveware**), coût moyen du downtime IT : 5 600 USD/minute (Gartner***).*

**Statista (2024) - 24 jours d'arrêt moyen (données issues d'enquêtes sur la durée moyenne d'interruption après une attaque ransomware)*
***Coveware (2020) - 21 jours d'arrêt moyen (Coveware Q4 2020 Ransomware Marketplace Report)*
****Gartner (2014) - coût moyen du downtime IT estimé à 5 600 USD par minute (Gartner IT Downtime Cost Study)*

Pour **déclencher la prise de conscience sur les risques cyber autour de la trésorerie**, les équipes doivent permettre à chacun d'en prendre la mesure. Or, chiffrer précisément l'impact financier d'un blocage cyber de la trésorerie pour bâtir un business case semble difficile à ce stade. Les impacts d'un arrêt de production sont souvent chiffrés par l'entreprise notamment à travers les Business Impact Analysis réalisés par l'équipe cyber, on peut aussi se baser sur la durée moyenne d'une crise cyber (21 jours, selon Gartner) appliquée au revenu quotidien de l'entreprise, mais il n'y a pas de volet spécifique « trésorerie».

> Dans ces conditions, une liste des effets potentiellement dévastateurs d'une attaque cyber spécifiquement sur la trésorerie donne une idée claire des enjeux.

- Risques sur la supply chain et le paiement des fournisseurs (risque de perte de confiance, voire de rupture, avec des fournisseurs critiques)
- Risques sur les ventes et les parts de marché du fait de livraisons impossibles (paiement impossible des transporteurs, retailers, et autres intermédiaires indispensables à l'acte de vente)
- Impact légal avec des situations de non-respect des contrats commerciaux et financiers
- Risque social majeur en cas de rupture des paiements essentiels, notamment des salaires, dont la visibilité interne en fait un puissant levier de prise de conscience
- Risques de réputation et menaces sur l'assurabilité de l'entreprise (en revanche une protection efficace renforce la puissance de négociation face aux assureurs).

MOBILISER L'ENSEMBLE DES ACTEURS, IDENTIFIER LES PROCESSUS ET FOURNISSEURS CRITIQUES

Avec une telle liste, chacun comprendra que la protection de la trésorerie doit sortir de la sphère strictement «finance» pour mobiliser l'ensemble de l'entreprise sur deux tâches essentielles : identifier les processus critiques et les fournisseurs indispensables à protéger en priorité.

Rassembler l'ensemble des acteurs passe par l'information des parties prenantes sur le rôle de la trésorerie via la description des processus financiers de bout en bout.

L'autre point clé reste de bien veiller au respect de chacune des compétences de l'entreprise. Le trésorier ne doit pas s'improviser expert cyber au risque de contrarier la DSI ou la direction cyber (en fonction des organisations), partenaires identifiés comme indispensables à la mise en place d'une protection efficace.

RECOMMANDATIONS

- **Construire et exposer des situations de crise concrètes** est un levier efficace et les simulations de crise de trésorerie, quand elles sont possibles, produisent des effets convaincants.
- **Se tourner vers d'autres entreprises partenaires** pour d'éventuels retours d'expériences.
- La question des **primes d'assurances** est identifiée comme un point d'entrée pour une discussion avec les achats.
- Il semble nécessaire de se livrer à une forme de géopolitique de l'entreprise pour identifier la direction la plus puissante auprès du comex (hors finances).
- **Identifier des gains pour chacune des parties prenantes**, notamment à travers les opportunités de transformation.
- Pour les équipes IT, l'argument le plus important est qu'une trésorerie qui fonctionne malgré l'attaque leur permet de se concentrer sur la restauration de la production.

LEVIER DE TRANSFORMATION

C'est un aspect à ne surtout pas négliger pour bâtir un business case de protection de la trésorerie et déclencher les investissements

La protection de la trésorerie et la mise en place de solutions de back up pour pallier les blocages d'une attaque cyber implique une cartographie complète des systèmes et des applications utilisées par l'entreprise.

Lors d'une telle revue de détail, en moyenne 30% des applications, 50% des reporting s'avèrent sans intérêt réel, les économies potentielles tirées de ce constat financent souvent largement la protection de la trésorerie.

L'identification fine des processus critiques peut amener à une protection plus efficace de l'ensemble de la chaîne de production

De même, la revue de détail des processus permet d'identifier les « golden data » qui seront des leviers de création de valeur.

Astran

ŒIL D'EXPERT #1

L'enjeu n'est pas de maintenir l'ensemble des activités, mais d'identifier ce qui doit impérativement continuer à fonctionner pour assurer la survie de l'entreprise.

Les travaux de la Taskforce montrent que la trésorerie apparaît, à ce titre, comme l'un des processus les plus critiques. Cette approche s'inscrit dans la notion de **Minimum Viable Company** (MVC) : un périmètre restreint de processus et de données à préserver en toutes circonstances.

La définition de ce MVC permet de prioriser les efforts, d'anticiper les crises et d'organiser un fonctionnement dégradé mais maîtrisé, condition essentielle de la résilience de la trésorerie et des entreprises.

INTERVIEW

THIERRY **REVAH**

Director Financing & Treasury TP

> TP anciennement Teleperformance est le leader mondial de la relation client externalisée, implanté dans le monde entier, avec des enjeux considérables de réponses en temps réel aux demandes des clients et un capital humain très important (autour de 500.000 salariés). Cela rend sans doute encore plus critiques les enjeux liés à la trésorerie, et ma première question découle de ce constat : est-ce que les menaces sur la trésorerie sont traitées par les équipes cyber au même titre que celles qui pèsent directement sur la production ?

Je dirais que les récentes attaques cyber, de plus en plus spectaculaires, comme celles qui ont frappé Jaguar et Marks & Spencer, ne font que renforcer la sensibilité du comité exécutif et des dirigeants du groupe face à ces risques. En raison de la nature même de notre activité, nous sommes déjà très conscients de ces menaces, mais il est crucial que nous restions vigilants et proactifs.

En ce qui concerne spécifiquement la trésorerie, nous faisons face aujourd'hui à des tentatives de fraude de plus en plus sophistiquées, notamment des «deep fakes» de sessions Teams, parfaitement réalisées, où l'on voit notre CEO demander tel ou tel virement vers tel ou tel pays, souvent la Chine. Cela nous arrive plusieurs fois par semaine.

> La sophistication est telle, que la mobilisation et les communications nécessaires pour y résister sont maintenant gérées par les équipes cyber, alors qu'avant la trésorerie pouvait s'en occuper seule.

Je connais mes limites, je ne peux plus assumer un tel déluge d'attaques et une telle sophistication, et c'est un point que je crois très important dans notre discussion : **pour organiser la protection de la trésorerie, il faut impliquer l'ensemble de l'entreprise.**

L'autre point, c'est qu'il faut des outils sophistiqués, ce qui nous amène à la question des investissements.

Effectivement, c'était au cœur des discussions de notre communauté, comment construire un business case suffisamment solide pour obtenir les moyens d'investir ?

Je dirais qu'il faut surtout commencer par ne pas parler de budget ! Notre groupe de travail a fait le constat qu'il était quasi impossible de chiffrer l'impact financier d'une paralysie de la trésorerie. Et, tant mieux, parce que cela permet de se concentrer sur les conséquences réelles, et elles sont dévastatrices.

En ce qui concerne TP, c'est le non-paiement des salaires qui entraîne des situations très graves, très vite. Cela nous est arrivé, à cause de problèmes techniques dans certains pays, d'avoir un ou deux jours de retard sur la paye, et bien la grève a été immédiate, et aussi rapidement, nos clients, qui ont besoin de réponses en temps réel, basculent leur trafic sur les plateformes concurrentes, tout cela va très vite.

Je dois dire aussi que j'ai été impressionné par la panne d'électricité géante en Espagne. Et là les solutions sont assez simples à formuler : décentraliser, garder la capacité d'agir en différents points du globe pour faire face à un tel incident. Simple à formuler, mais complexe à réaliser, et c'est donc un gros chantier que nous sommes en train d'entreprendre.

Et pour revenir sur la négociation des budgets, j'insiste sur le fait qu'il ne faut pas aller chercher un ROI, mais bien plus considérer qu'il s'agit d'une sorte de prime d'assurance permettant la continuité de l'activité.

> Parce que les enjeux sont trop importants

Exactement ! Et j'ajoute la possibilité de transformation, que j'ai découverte grâce à nos échanges. Quels sont nos processus réellement critiques ? J'avoue qu'on ne s'était pas réellement posé la question, nous allons le faire et je crois que les réponses seront très instructives, en prévision, justement, d'une réunion avec les équipes IT.

Mais au-delà, je tiens à me tenir informé sur la marche du monde, sur l'évolution des menaces, j'en discute avec nos experts, qui me parlent d'une attaque qui pourrait être paralysante non pas comme une possibilité éventuelle, mais comme une évidence qu'il faudra forcément affronter un jour, comme disent les Anglo-saxons ce n'est pas le «if» mais le «when».

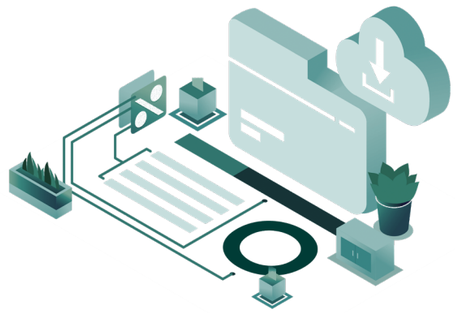
Face à cela, je suis d'accord avec les conclusions du rapport, **nous ne pouvons pas nous contenter d'attendre, il faut se préparer efficacement, et c'est pourquoi je pense fermement que les décisions et les communications concernant ces questions doivent être prises au niveau du comité exécutif.** En d'autres termes, la protection de nos organisations sur ce sujet doit venir de l'équipe managériale pour garantir une mobilisation de tous.

THIERRY REVAH

WORKSHOP #2

ASSURER LA CONTINUITÉ OPÉRATIONNELLE DE LA TRÉSORERIE : PROCESSUS CRITIQUES, DISPONIBILITÉ ET QUALITÉ DES DONNÉES, RELATIONS BANCAIRES

Les travaux de la Taskforce mettent en évidence que la résilience de la trésorerie en situation de crise cyber repose d'abord sur la capacité de l'équipe trésorerie à agir de manière autonome et immédiate.



Certains processus doivent pouvoir être exécutés en situation de crise, indépendamment des autres fonctions, afin de préserver les engagements financiers essentiels de l'entreprise. Parmi eux, **le paiement des salaires** apparaît comme un processus vital prioritaire, en raison de ses impacts sociaux directs et de sa forte visibilité interne.

La Taskforce souligne également l'importance de sécuriser le **paiement des fournisseurs critiques** tout au long de la crise, dans un contexte de chaînes d'approvisionnement déjà fragilisées. Cette continuité suppose une identification et une priorisation réalisées en amont, en lien étroit avec les achats et les métiers, et fondées sur une analyse claire des impacts dans le temps.

Une hiérarchisation partagée est indispensable pour permettre des décisions rapides et cohérentes dès les premières phases de la crise.

Un certain nombre d'autres processus dits de **trésorerie (service de la dette, dénouement des opérations de marché, titrisation)** peuvent être perçus comme plus techniques par la direction générale mais n'en sont pas moins critiques pour l'entreprise et son financement.

Enfin, la résilience de la trésorerie repose sur la robustesse des **relations bancaires** et la disponibilité des **données critiques.** La Taskforce met en avant la nécessité d'intégrer les partenaires bancaires au dispositif de gestion de crise et de sécuriser l'accès aux données essentielles de trésorerie dans des environnements indépendants et exploitables en mode dégradé. Ces éléments constituent des leviers structurants pour maintenir la capacité d'action pendant la crise et préparer un retour à la normale maîtrisé.

SALARIÉS : SÉCURISER LE PROCESSUS DE PAIE

La question du paiement des salaires constitue un enjeu central en situation de crise, en raison des impacts sociaux immédiats et de la forte visibilité interne. Dans ce contexte, la Taskforce souligne que la capacité à exécuter la paie de manière fiable et sécurisée, y compris en environnement dégradé, est un facteur clé de stabilité et de maîtrise de la crise.

La sécurisation du processus de paie suppose une préparation en amont, incluant l'identification des dépendances critiques (données de paie, circuits de validation, relations bancaires), ainsi que la définition de modalités de fonctionnement de secours. La capacité à s'appuyer sur des données de référence récentes, préalablement sécurisées et accessibles, et à mobiliser rapidement les acteurs concernés est essentielle pour garantir la continuité des engagements de l'entreprise envers ses salariés.

Le paiement des salaires constitue un point de visibilité majeur au sein des entreprises et peut devenir un levier déterminant pour sensibiliser la direction générale et les métiers à la nécessité d'investir dans la protection de la trésorerie face au risque cyber.

FOURNISSEURS CRITIQUES : MAINTENIR LA RELATION

Les relations fournisseurs sont profondément affectées par les tensions géopolitiques et les ruptures d'approvisionnement parfois brutales qui peuvent, à elles seules, bloquer l'ensemble du processus de production. Dans ce contexte, la Taskforce souligne que la capacité à maintenir le paiement des fournisseurs pendant une crise constitue un atout décisif, tant pour limiter les impacts immédiats que pour accélérer la phase de reprise.

La définition des fournisseurs critiques demeure complexe, et ne peut être uniforme à l'échelle de l'entreprise, d'où l'importance d'établir en amont, avec les métiers, une liste de priorités claires et partagées : fournisseurs indispensables à la continuité opérationnelle (par exemple, certaines plateformes cloud), fournisseurs fragiles, etc. **Ce travail doit être régulièrement mis à jour afin d'éviter toute ambiguïté décisionnelle en situation de crise.** Les taxes et impôts peuvent, le cas échéant, être intégrés dans cette liste de fournisseurs critiques.

Dans une crise, tout est critique pour tout le monde, et donc pour définir une liste de priorités il faut absolument une hiérarchie des urgences, liée à la temporalité des différents impacts sur les parties prenantes.

PROCESSUS DE TRÉSORERIE : PRÉSERVER LA CAPACITÉ D'ACTION FINANCIÈRE

Certains processus de trésorerie – hors paiements des salariés et fournisseurs critiques – constituent un socle indispensable à la continuité financière de l'entreprise (service de la dette, opérations de marché, couvertures financières, etc). La Taskforce souligne qu'en situation de crise, leur interruption peut entraîner des conséquences immédiates en matière de liquidité, de respect d'engagements contractuels et de crédibilité financière auprès des partenaires bancaires et des marchés.

Cela implique la définition, en amont, de modalités de fonctionnement de secours permettant d'assurer la continuité des opérations essentielles à J ou J+1, indépendamment de la disponibilité des outils de gestion habituels.

Ce qui est très important pendant une crise cyber c'est d'être capable de faire vivre les données business et les données de paiement et s'assurer ensuite que l'on sait exactement ce qui a été traité ou payé via ces canaux secondaires.

RELATIONS BANCAIRES : UN LIEN STRATÉGIQUE

La continuité des flux de trésorerie en situation de crise repose avant tout sur la capacité à activer des circuits de paiement opérationnels et sur la qualité des relations bancaires.

À ce titre, les travaux de la Taskforce montrent que la seule disponibilité des outils de gestion (TMS), y compris lorsqu'ils sont hébergés dans le cloud, ne suffit pas à garantir la capacité d'action de la trésorerie. En cas de crise cyber majeure, l'indisponibilité des systèmes d'authentification ou des dispositifs de validation peut rendre ces outils inaccessibles, même lorsqu'ils demeurent techniquement opérationnels. **La mise en place de dispositifs annexes et indépendants est alors indispensable pour maintenir une capacité minimale d'action sur les flux critiques.**

Dans ce cadre, plusieurs prérequis apparaissent indispensables :

- Partager **le plan de crise avec les banques** qui seront appelées à intervenir
- Tester régulièrement les **solutions de web banking de secours** (lorsqu'elles existent)
- Différencier clairement les **banques de paiement et les banques d'encaissement**
- Conserver les **coordonnées bancaires strictement critiques** dans un espace de stockage indépendant, sécurisé et accessible en situation dégradée, le recours exclusif au support papier ayant montré ses limites opérationnelles.

La question clé reste de savoir s'il convient de confier l'intégralité de la gestion de crise à une seule banque ou de s'appuyer sur plusieurs banques partenaires. D'après la Taskforce, le recours à une banque unique présente des risques en matière de vulnérabilité et de confidentialité et doit, à ce titre, être écarté.

Il apparaît préférable de s'appuyer sur un nombre restreint de partenaires bancaires, sélectionnés en amont, formés aux procédures de gestion de crise et avec lesquels des dispositifs de paiement de secours auront été formalisés.

MESURER LA GRAVITÉ D'UNE CRISE

Au cœur de la gestion d'une crise cyber touchant la trésorerie, la construction d'une échelle de gravité dans le temps apparaît indispensable : qui est concerné ? Et qui faut-il servir en priorité dans les premières heures, puis les premiers jours, voire plus en fonction de la durée de la crise ?

Dans ces conditions, la liste des processus et fournisseurs critiques dépend d'abord du moment précis où ils seraient impactés. De même, le moment du déclenchement d'un plan d'action de crise dépendra de l'urgence à payer les salaires, honorer les dettes ou soutenir des fournisseurs fragilisés par un arrêt des paiements. **L'estimation rapide et fiable de la durée de la crise constitue un élément fondamental de la prise de décision et conditionne le niveau de mobilisation des différentes parties prenantes internes et externes.**

La protection de la trésorerie contre une crise cyber permet d'élargir le périmètre de travail au-delà des trésoriers pour intégrer les fonctions comptabilité fournisseurs, achats et P2P, indispensables à l'identification des fournisseurs critiques.

La protection de la trésorerie permet de faire évoluer la culture interne et de passer d'une logique de conformité des processus à une logique de réelle protection du business.

Le paiement des salariés est un enjeu majeur sur lequel aucun compromis n'est envisageable.

L'ENJEU DE LA PROTECTION DES DONNÉES DE TRÉSORERIE

La définition des données critiques découle directement du travail d'identification des processus critiques. L'objectif n'est pas de conserver l'ensemble des données, mais de se limiter à celles strictement indispensables au maintien de l'activité.

L'identification des données critiques doit s'appuyer sur un travail partagé entre les parties prenantes, puis être complétée par une évaluation de leur qualité. Celles-ci doivent ensuite être exportées vers un environnement indépendant, sécurisé, garantissant disponibilité et confidentialité. Ces données étant par nature dynamiques, leur mise à jour régulière est indispensable. Il convient également d'identifier un contact clé sur chacun des processus critiques et de disposer d'un moyen fiable de le joindre en toute circonstance.

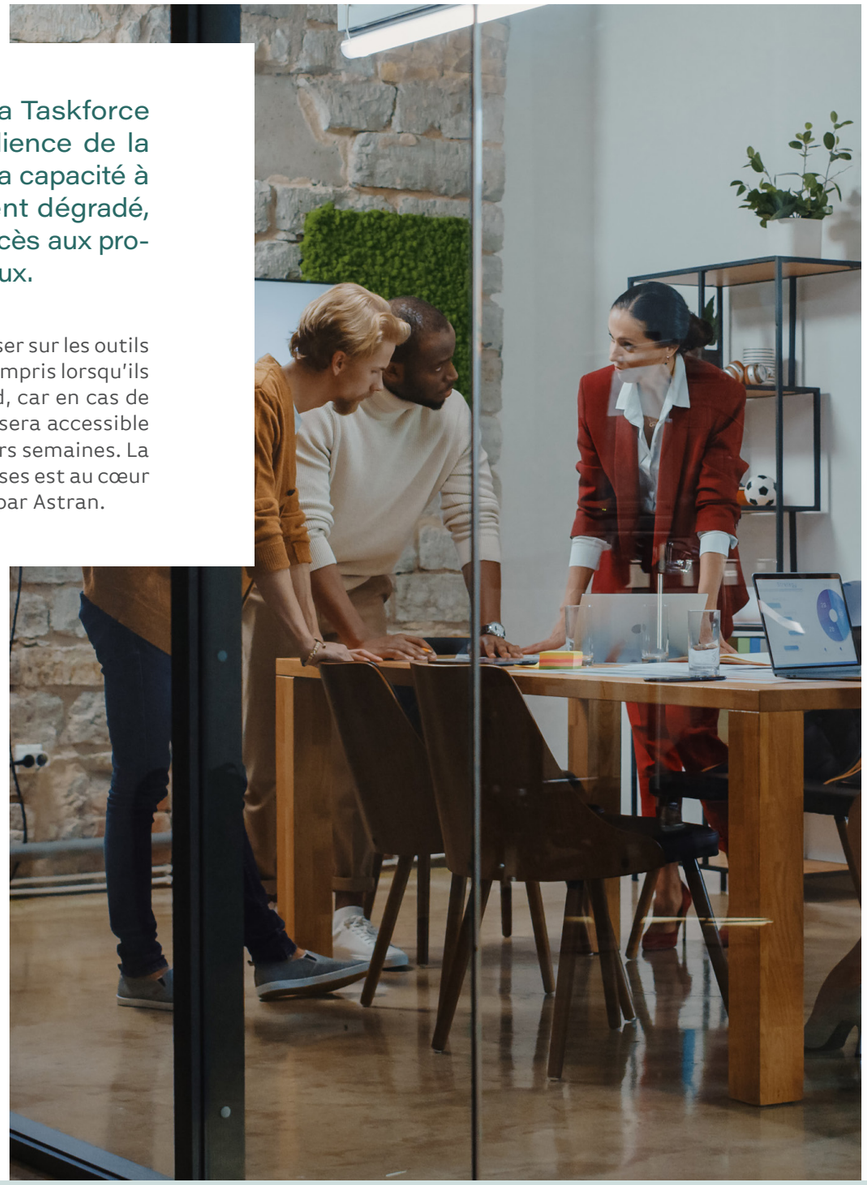
Enfin, la poursuite de l'activité pendant la crise impose de pouvoir intégrer les nouvelles données produites et d'en garantir la compatibilité et l'auditabilité lors de leur réintégration dans les systèmes d'information.

Astran

ŒIL D'EXPERT #2

Les conclusions de la Taskforce montrent que la résilience de la trésorerie repose sur la capacité à agir en environnement dégradé, et pour cela à avoir accès aux processus et données vitaux.

Cette capacité ne peut reposer sur les outils de gestion quotidienne, y compris lorsqu'ils sont hébergés dans le cloud, car en cas de crise majeure plus rien ne sera accessible au trésorier pendant plusieurs semaines. La disponibilité pendant les crises est au cœur de la technologie brevetée par Astran.



CONCLUSION

DÉMARRER CONCRÈTEMENT UN PROGRAMME DE RÉSILIENCE DE LA TRÉSORERIE

Les travaux de la Taskforce aboutissent à des principes clés permettant d'initier efficacement un programme de résilience de la trésorerie.

1 Partir de l'hypothèse de la rupturetotale

Considérer qu'en cas de crise majeure (notamment d'origine cyber), les outils de gestion, les systèmes d'authentification et les accès habituels peuvent être indisponibles, y compris sur les logiciels hébergés dans le cloud.

2 Prioriser un nombre limité de processus vitaux

Adopter une approche MVC (Minimum Viable Company) en concentrant les efforts sur un périmètre restreint de processus indispensables à la continuité financière, sans chercher à couvrir l'ensemble des activités financières.

Cette priorisation doit également intégrer les régions, entités ou équipes indispensables à l'exécution de ces processus en situation de crise.

3 S'appuyer sur un nombre d'acteur limités

Impliquer dès le départ un nombre limité d'intervenants clairement identifiés : CISO, IT, contrôle interne, trésorerie, et, le cas échéant, partenaires bancaires.

4 Démarrer par un processus de bout en bout

Traiter un premier processus de manière complète (processus simplifié, données vitales, acteurs opérationnels) afin d'illustrer la valeur de la démarche et de créer un premier succès mobilisateur.

5 Tester régulièrement par des exercices ciblés

Organiser des micro-exercices de crise, impliquant uniquement les acteurs opérationnels afin de valider le dispositif de résilience et d'ancrer durablement les bons réflexes.

A PROPOS D'ASTRAN

Astran accompagne les organisations dans le renforcement de leur résilience opérationnelle face aux crises majeures, notamment d'origine cyber, à travers la définition de leur Minimum Viable Company (MVC).

Sa plateforme AlwaysReady®, collaborative et adaptable, permet de structurer et d'ajuster en continu les priorités des organisations, les processus critiques, les données vitales et les modes de fonctionnement dégradés, en fédérant l'ensemble des parties prenantes.

CONTACT

Yosra JARRAYA
ASTRAN
CEO et Co-founder
yosra.jarraya@astran.ai

Gilles SEGHAIER
ASTRAN
Chief Product Officer
et Co-founder
gilles.seghaier@astram.ai

Yahya JARRAYA
ASTRAN
Chief Customer Officer
et Co-founder
yahya.jarraya@astran.ai

Céline COIFFÉ
LOSAM
Responsable de la Taskforce
celine@insignts.futureoffinance.fr


Astran


LOSAM