PURESTORAGE®
Uncomplicate Data Storage, Forever

LIVRE BLANC

Renforcer la résilience opérationnelle des services financiers

Solutions de gestion des nouvelles réglementations relatives aux risques

Sommaire

« 90 % des spécialistes de la résilience s'attendent à une augmentation des menaces visant leur organisation au cours des trois prochaines années. »

THE CONFERENCE BOARD,
AOÛT 2023[1]

Introduction

Pour les sociétés de services financiers, la gestion des risques est une responsabilité qui ne cesse de s'accroître et d'évoluer. Depuis le choc financier de 2007-2008, les ministres des finances et les autorités de réglementation des différents pays ont constamment renforcé les normes en matière de gestion des risques et inclus de plus en plus de domaines dans leurs définitions des activités couvertes. Dans le même temps, l'arrivée de nouvelles technologies et les évolutions du marché ont multiplié les défis à relever par les entreprises pour garantir leur résilience opérationnelle.

Les autorités de réglementation et le marché en général ont fini par admettre qu'un écosystème de services financiers de plus en plus vaste, complexe et interconnecté nécessite une extension de la gestion des risques allant bien au-delà des mesures strictement financières pour inclure toutes les opérations et l'écosystème qui les englobe. La gestion des risques du 21e siècle couvre de plus en plus tous les aspects d'une opération, en mettant l'accent sur les données et la technologie qui sont à la base des activités commerciales modernes. La résilience opérationnelle va devenir un domaine incontournable que les entreprises devront gérer et préserver avec discipline et diligence, et pas uniquement parce qu'il s'agit d'une nécessité imposée par les autorités de réglementation. En effet, la résilience opérationnelle offre de multiples avantages à une entreprise, notamment en lui permettant de prouver à ses clients et aux autres parties prenantes que son activité commerciale est sécurisée (à l'instar de leur investissement), de se distinguer de la concurrence et d'assurer sa stabilité face aux pertes, aux échecs ou à l'instabilité de l'emploi. La résilience opérationnelle est un élément essentiel pour les entreprises modernes.

Elle désigne la capacité des entreprises, des infrastructures des marchés financiers et du secteur dans son ensemble à préserver ou à restaurer leurs opérations et services en cas d'interruptions, sinistres ou autres risques opérationnels. Plus largement, elle englobe les stratégies, processus et systèmes que les institutions financières mettent en place afin de garantir la continuité de leurs services stratégiques pour leurs clients en toutes circonstances. La résilience opérationnelle est devenue de plus en plus importante pour les sociétés de services financiers qui doivent faire face à un nombre croissant de risques, notamment aux cyberattaques, attaques de ransomware, catastrophes naturelles et autres pandémies.

Examiner ce problème complexe du point de vue des autorités de réglementation peut s'avérer utile pour comprendre la résilience opérationnelle des services financiers. En étudiant l'état actuel de la réglementation et en creusant la question, il est possible d'observer les similitudes et les différences entre les régions géographiques, les domaines sur lesquels les autorités de réglementation concentrent toute leur attention, ainsi que les défis et les approches pertinentes pour gérer ce problème délicat. On obtient au final une image assez précise des enjeux autour de la résilience opérationnelle.

Perspectives mondiales en matière de résilience opérationnelle des services financiers

La résilience opérationnelle en tant que responsabilité et fonction de gestion des risques est un phénomène relativement récent. Alors que le domaine connexe de la planification de la continuité des opérations remonte aux années 70 (voir encadré), la résilience opérationnelle est passée au premier plan en 2017. Face à l'augmentation des incidents liés à la cybersécurité et à la propagation des attaques de ransomware, les autorités de réglementation en Europe, à Singapour, à Hong Kong, aux États-Unis et dans de nombreux autres pays ont reconnu que la gestion des risques des entreprises nécessitait d'aller au-delà des mesures financières pour englober tous les aspects des opérations, notamment parce que les technologies de l'information et des communications (TIC) sont désormais la pierre angulaire de l'entreprise moderne. Logiquement, la cyberrésilience au centre de cette démarche est une préoccupation majeure parmi de très nombreuses questions cruciales, alors que les autorités de réglementation et les entreprises reconnaissent les liens et concentrations qui ont donné naissance au concept « Trop gros pour faire faillite » de la crise financière mondiale. En réalité, l'augmentation des concentrations et le recours accru aux opérations numériques n'ont fait que durcir les enjeux.

Depuis 2017, la résilience opérationnelle a poursuivi son évolution hétérogène, chaque autorité venant apporter une réponse différente en termes de réglementation. Cette approche inégale et l'adoption des mesures qui en découlent se reflètent dans la manière dont les entreprises privées ont relevé ce défi et sont un bon indicateur du développement de cette question à l'avenir.

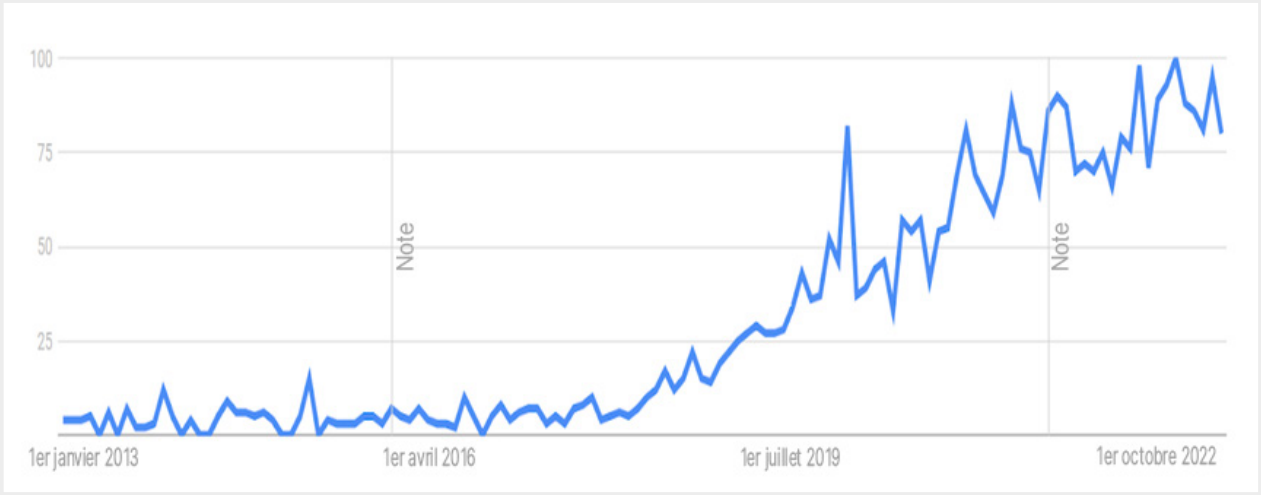

FIGURE 1 Source : Google Trends : « Where there's smoke there's fire: internet searches for "operational resilience" increased dramatically beginning in 2018 » (Il n'y a pas de fumée sans feu : forte augmentation des recherches de l'expression « Résilience opérationnelle » sur Internet depuis 2018)

En résumé, alors que la question de la résilience opérationnelle a commencé à se poser pour toutes les autorités de réglementation internationales à partir du milieu des années 2010, son approche est très différente selon les régions géographiques spécifiques et le rythme de mise en œuvre des mesures appropriées varie aussi considérablement. Plus précisément, l'UE et le Royaume-Uni sont en avance en termes de calendriers de mise en œuvre et de caractère normatif des réglementations, tandis que les États-Unis ont adopté une approche plus collaborative, mais incohérente, et que le sérieux des initiatives prises en Asie-Pacifique dépend des régimes politiques des différents pays.

UE et Royaume-Uni

- L'UE a adopté les réglementations les plus ambitieuses et normatives en matière de résilience opérationnelle. Une première version de la réglementation DORA (Digital Operational Resilience Act) a été publiée en septembre 2020 et cette loi entrera en vigueur dès le 17 janvier 2025. La réglementation DORA a été élaborée à partir des 12 principes de la résilience opérationnelle publiés en 2021 qui reposent sur les principes de gestion du risque opérationnel du Comité de Bâle sur le contrôle bancaire publiés en 2011 et révisés en 2014 et 2021.[2] Il s'agit d'un cadre global unifiant les processus et normes du secteur financier, qui garantit que tous les acteurs du

système financier, y compris les fintechs et les prestataires de services tiers, sont soumis à un ensemble de normes communes afin de limiter les risques liés aux technologies de l'information et des communications pour leurs opérations.
Les aspects essentiels de la réglementation DORA incluent la mise en place et le maintien continu de règles de sécurité, de cadres et principes de gestion des risques, de formations performantes et actives en matière de sensibilisation des utilisateurs, d'audits et de tests réguliers des processus et systèmes de sécurité. Même si la réglementation DORA ne prévoit pas explicitement d'amendes ou de sanctions, les différents pays membres de l'UE peuvent imposer des pénalités et des sanctions pénales pouvant inclure des amendes allant jusqu'à 2 % du chiffre d'affaires annuel total d'une entreprise.

Pour en savoir plus sur cette réglementation, consultez l'article suivant sur notre blog : « How Banks Benefit from the New Digital Operations Resilience Act » (Comment les banques peuvent tirer parti de la nouvelle réglementation Digital Operations Resilience Act)

- Le Royaume-Uni s'est également beaucoup impliqué dans l'élaboration et l'adoption de directives sur la résilience opérationnelle et a notamment infligé à une banque britannique une amende de 50 millions de livres sterling pour un incident relatif à la résilience opérationnelle en décembre 2022.[3] Face à la sensibilisation accrue aux cybervulnérabilités, la Financial Conduct Authority (FCA), la Banque d'Angleterre et la Prudential Regulation Authority (PRA) ont promulgué leur propre politique en matière de résilience opérationnelle en mars 2021. Cette politique souligne la nécessité d'améliorer la résilience des sociétés financières aux interruptions opérationnelles et les oblige à établir des plans pour gérer ces risques graves, mais plausibles. Les dispositions de cette politique sont entrées en vigueur en avril 2022 et les entreprises disposent d'une période de transition de trois ans jusqu'en 2025 pour se mettre en conformité avec les directives de leur plan.

  En substance, ces réglementations obligent les entreprises à définir et à soutenir des services métier stratégiques et à déterminer les niveaux de perturbations qu'elles peuvent subir tout en continuant à assurer leurs services essentiels. Les entreprises doivent alors réaliser des tests de configuration et de scénarios mettant l'accent sur la stratégie de communication et les capacités internes en matière d'auto-évaluation des performances, notamment concernant l'identification des faiblesses ou des vulnérabilités.

  En résumé, les priorités de la FCA, de la Banque d'Angleterre et de la PRA sont la prévention, l'adaptation, la gestion, la reprise et l'apprentissage face aux interruptions opérationnelles.

L'approche américaine

- Contrairement à l'UE et au Royaume-Uni, le développement de la résilience opérationnelle aux États-Unis a été basé sur une approche consultative ascendante et une coopération interagences, plutôt que sur une réglementation descendante. La Cybersecurity and Infrastructure Security Agency (CISA) est au cœur de cette approche. Cette agence créée en 2018 fait partie du Département de la Sécurité intérieure des États-Unis. Les responsabilités de la CISA incluent l'évaluation des risques, la réduction des vulnérabilités, la détection des menaces, la réponse aux incidents et les initiatives de reprise. Pour assurer ces missions, elle collabore avec d'autres agences fédérales, collectivités publiques locales et nationales, et des entreprises du secteur privé. La CISA met l'accent sur la collaboration volontaire et la mise à disposition de ressources telles que des outils de gestion des risques, d'évaluation des menaces et de formation afin de renforcer l'infrastructure américaine et d'aider les différentes entités à améliorer leur cybersécurité.
- Aux États-Unis, certaines responsabilités incombent également au FFIEC (Federal Financial Institutions Examination Council), une institution gouvernementale qui a un mandat élargi, mais moins spécifique. Il s'agit d'un organisme interagences composé des dirigeants des cinq agences fédérales chargées des questions bancaires : le Conseil des gouverneurs de la Réserve fédérale des États-Unis, la Société fédérale d'assurance-dépôts (Federal Deposit Insurance Corporation), l'Administration nationale des coopératives de crédit (National Credit Union Administration), le Bureau du contrôleur de la monnaie (Office of the Comptroller of the Currency) et le Bureau de protection des consommateurs en matière financière (Consumer Financial Protection Bureau). En général, son rôle est d'assurer une bonne coordination entre les agences et de proposer des conseils, et non d'imposer une réglementation en tant que telle. La Securities and Exchange Commission (SEC) et la Commodity Futures Trading Commission (CFTC) examinent également les pratiques des entreprises en matière de résilience opérationnelle, ainsi que leur capacité à prévenir les interruptions des services stratégiques et à protéger les données, les documents et les actifs des investisseurs.

Plus récemment, la Maison-Blanche a publié une stratégie de cybersécurité nationale au printemps 2023. Cette stratégie propose une mission élargie qui va bien au-delà des marchés financiers pour inclure des domaines tels que les infrastructures énergétiques et les systèmes de santé. À l'instar de la plupart des autres initiatives prises aux États-Unis, elle s'appuie davantage sur la coopération que sur la réglementation.

Approches adoptées en Asie-Pacifique

- En Asie-Pacifique, Singapour et Hong Kong ont été les pays les plus actifs au niveau de la mise en place de pratiques de résilience opérationnelle, tandis que d'autres places financières importantes, notamment l'Australie, le Japon et la Malaisie, répondent aux exigences en matière de cybersécurité, mais avec une approche plus limitée ou prudente.
- L'Autorité monétaire de Singapour (Monetary Authority of Singapore) a d'abord présenté des directives relatives à la gestion de la continuité des opérations début 2003, puis a continué à étendre et à affiner son approche au fil des années. Des directives révisées bien plus proches des paramètres de résilience opérationnelle plus stricts et complets ont été finalisées en juin 2022 et les institutions financières sont désormais priées de s'y conformer. Elles doivent remettre un plan conforme aux exigences réglementaires ainsi qu'un programme d'audit d'ici juin 2023 et un premier audit doit être réalisé d'ici juin 2024.

  Pour se conformer à ces directives, une institution financière doit adopter une vue globale de bout en bout des dépendances des services métier stratégiques tenant compte de l'ensemble global des processus impliqués. Même si des concepts relatifs à la continuité des opérations tels que les délais de récupération des services sont imposés, les réglementations tiennent également compte de la complexité créée par les relations cruciales avec les tiers et le fait que certains aspects des services doivent passer avant d'autres considérations lors du long processus de reprise par étapes.
- L'Autorité monétaire de Hong Kong (Hong Kong Monetary Authority) a publié une circulaire relative à la résilience opérationnelle intitulée « OR-2 Supervisory Policy Manual » (Manuel de politique de surveillance OR-2) en mai 2022, harmonisée avec les normes de la Banque des règlements internationaux (BIS) promulguées en 2021. La première phase de la nouvelle réglementation qui s'est terminée en mai 2023 incluait la nécessité de définir un cadre pour la résilience opérationnelle, ainsi qu'un calendrier de mise en conformité. La seconde phase court jusqu'en mai 2026, date à laquelle les institutions financières devront totalement respecter leurs plans de résilience opérationnelle.

  La circulaire OR-2 oblige les institutions « à réaliser des tests de scénarios pour des incidents graves, mais plausibles, à établir des stratégies de gestion des risques plus complètes et des cadres spécifiques aux opérations métier stratégiques identifiées, et à mettre en œuvre des programmes de gestion des incidents stables, dont les exigences vont bien au-delà des cadres actuels relatifs à la planification de la continuité des opérations et à la gestion des risques opérationnels. Les institutions financières doivent prouver par le biais de plans de tests et de rapports qu'elles ont véritablement défini et mis en œuvre des scénarios capables d'évaluer les opérations stratégiques de manière appropriée. »[4]

« Les interruptions opérationnelles peuvent causer de vastes préjudices aux consommateurs, présentent un risque pour l'intégrité du marché, menacent la viabilité des entreprises et provoquent l'instabilité du système financier. »

FCA, INSTANCE DE RÉGULATION BRITANNIQUE[5]

Points importants à retenir concernant les approches de la résilience opérationnelle au niveau international

Compte tenu de la complexité et de la diversité des approches adoptées par les autorités de réglementation internationales concernant la résilience opérationnelle, une société de services financiers pourrait choisir la solution de facilité en n'examinant que les réglementations qui s'appliquent directement à sa région ou zone géographique spécifique. Cette approche trop simpliste pourrait s'avérer inappropriée, car certaines réglementations peuvent avoir des effets sur un territoire extérieur et en affecter d'autres. La réglementation DORA, par exemple, s'applique à toutes les sociétés de services financiers menant des activités dans l'UE, notamment toutes les entreprises fournissant des services technologiques et de communication. Cette liste couvre les organismes de paiement, les fournisseurs de monnaie électronique, les prestataires de services relatifs aux informations comptables, les sociétés de gestion, les assureurs, les fournisseurs de services de données (y compris les services cloud et de datacenter) et les services liés au matériel. Le spectre des entreprises concernées est très vaste, ce qui est totalement inédit. Très vite, aucune entreprise ne pourra se soustraire à ses obligations découlant du champ d'application des réglementations et des mandats relatifs à la résilience opérationnelle.

Sachant cela, il est utile d'étudier les menaces courantes qui définissent les approches de la résilience opérationnelle au niveau international. Plus précisément, l'accent est mis sur une approche commune incluant la définition de normes de cybersécurité avec une mise en conformité et des tests obligatoires, sur le signalement des incidents et sur un vaste mandat visant à favoriser la résilience dans tous les secteurs d'activité stratégiques, et pas simplement au niveau des services financiers.

Analyse plus approfondie

La cybersécurité au centre de la stratégie

Les TIC ou le domaine cyber ne sont pas à l'origine de tous les problèmes liés à la résilience opérationnelle. Toutefois, ces derniers ont des conséquences sur la base technologique principale de l'entreprise moderne. C'est pourquoi la cybersécurité est essentielle à cette approche axée principalement sur la sensibilisation des utilisateurs et la préparation aux attaques de ransomware. L'émergence du ransomware-as-a-service en tant que modèle commercial et la croissance continue des ransomware parrainés par des États illustrent la manière dont cette menace continue d'évoluer et de prendre de l'ampleur. La portée des cyberattaques a également tendance à être plus grande et systématique par rapport aux défaillances opérationnelles conventionnelles. Les réparations et la reprise engendrées par ces incidents généralement bien plus médiatisés et coûteux sont susceptibles d'être considérablement plus longues.

Priorité à l'infrastructure et aux services stratégiques

Une ancienne approche de la continuité des opérations suivait un modèle de type « hautes murailles et douves profondes » qui ne faisait pas la différence entre les éléments opérationnels essentiels et secondaires. Cette approche n'est plus efficace (si tant est qu'elle le fut un jour) et doit être remplacée par une approche qui privilégie la préservation d'un maximum de fonctions métier en cas d'incident. Le plan correspondant doit être complet et flexible. Par exemple, il est désormais essentiel de faire la distinction entre des éléments stratégiques et secondaires d'une entreprise pour que les plans d'urgence puissent garantir la continuité des opérations de cette entreprise, même en cas de diminution de ses capacités.

Cadre de gestion des risques

Comme mentionné précédemment, la gestion des risques fut une mesure purement financière, mais ce temps-là est révolu. Le cadre de la gestion des risques s'est considérablement étendu pour inclure la résilience opérationnelle en tant que facteur nécessitant l'adoption de nouvelles approches innovantes au niveau de l'entreprise. L'ajout de facteurs de résilience aux mesures des risques financiers change radicalement l'orientation de l'analyse et augmente énormément l'ampleur des efforts déployés.

Coûts de la gestion des risques

Les coûts de la gestion des risques étaient auparavant mesurés strictement en termes d'exposition au marché avec des mesures comme la valeur à risque (VaR) ou l'ETL (Expected Tail Loss). Dans ce type d'approche, les meilleurs outils de gestion des risques étaient les outils les plus économiques. Dans le nouveau monde des réglementations favorisant la résilience opérationnelle, la gestion des risques est devenue bien plus complexe et variée, et les anciennes mesures des risques totalement obsolètes. À l'avenir, la complexité de la conformité sera telle que les coûts devront être mesurés en tenant compte des coûts par performance, et non simplement des coûts initiaux. Les outils devront être plus complets : une simple recherche de la solution la plus économique offrant le strict minimum ne suffira plus.

Directives et normes

On observe l'émergence progressive de directives et de normes qui définissent la résilience opérationnelle. Même si elles ne sont pas encore unifiées et optimisées, nous pourrons bientôt envisager l'élargissement et la codification de ces normes. De plus, les entreprises seront probablement davantage affectées par ces réglementations en dehors de leur territoire national. La réglementation DORA constitue le cadre réglementaire le plus développé, le plus normatif et probablement le plus performant. Il s'agit donc d'une norme efficace que la plupart des établissements de services financiers et des fournisseurs de technologies doivent respecter.

Observabilité

Une approche « loin des yeux, loin du cœur » est inappropriée en termes de gestion des risques. Toutefois, les solutions de surveillance traditionnelles, accumulées au fil des ans et dans divers silos, engendrent des zones d'ombre, des goulets d'étranglement au niveau des performances et une augmentation du délai moyen de réparation et ne répondent pas aux exigences rigoureuses des autorités de réglementation. Dans le cadre d'un plan de résilience global, les institutions financières doivent adopter une approche d'observabilité proactive leur permettant de surveiller en permanence les pipelines de données et d'utiliser des workflows automatisés pour détecter des anomalies, déclencher des alertes et améliorer l'atténuation des risques. Mieux vaut prévenir que guérir.

Signalement des incidents

Tout en prenant la mesure de l'évolution fulgurante des cybermenaces et de l'immaturité relative des programmes de résilience opérationnelle, les autorités de réglementation continuent à mettre l'accent sur le signalement rapide et complet des incidents à leur égard et à la communauté dans son ensemble. Le réflexe habituel de tout boucler et de tenir sa langue pendant et après un incident doit être abandonné. À l'avenir, la coopération et la transparence en matière de résilience opérationnelle doivent devenir la procédure standard à respecter.

Gestion des risques tiers

La continuité des opérations traditionnelle avait tendance à considérer l'entreprise comme une île, mais ce concept est désormais complètement dépassé grâce aux pratiques opérationnelles modernes. Les approches innovantes de la résilience opérationnelle intègrent le fait que la planification doit s'étendre vers l'extérieur de l'entreprise pour inclure les tiers qui représentent des sources de risques et des éléments essentiels dans le fonctionnement d'un écosystème financier.

Complexité

Il est d'ores et déjà évident que l'élargissement de la gestion des risques pour les services financiers incluant la résilience opérationnelle augmente considérablement la complexité de la tâche. Cela nécessite de nouvelles compétences et ressources, implique davantage de composantes de l'entreprise et accroît l'interconnexion des activités en raison des interdépendances, notamment celles impliquant des tiers. En outre, l'émergence de catégories d'actifs numériques comme les cryptomonnaies et le financement décentralisé, les perturbations liées aux changements climatiques ou les mandats relatifs aux enjeux sociaux, environnementaux et de gouvernance compliquent davantage la situation.

> « L'amélioration de la résilience opérationnelle présente d'immenses avantages qui dépassent largement les procédures formelles de conformité. »
>
> **GUY WARREN, PDG, ITRS**[6]

En résumé, la résilience opérationnelle est une discipline relativement nouvelle, mais elle va rapidement devenir un des domaines prioritaires incontournables pour les sociétés de services financiers. Alors que nous en sommes encore aux premières étapes de la définition de la résilience opérationnelle en tant que discipline de gestion des risques, il est important de réaliser que toutes les initiatives doivent être dynamiques, tout en évitant de les traiter comme des événements ponctuels. Un plan de résilience opérationnelle n'est jamais « terminé » : il doit être testé et faire l'objet d'un soutien actif et continu. Étant donné que les règles et les exigences sont de plus en plus codifiées et continueront d'évoluer avec les activités et les technologies, le résultat est évident : à l'avenir, toutes les institutions financières pourront tirer parti d'une approche et de pratiques complètes et performantes en matière de résilience opérationnelle.

Techniques favorisant la résilience opérationnelle

Par rapport aux approches conventionnelles de la cybersécurité ou de la continuité des opérations, la résilience opérationnelle est bien plus vaste et plus complexe. Elle admet la survenue très probable d'un incident et abandonne la vision purement défensive et préventive au profit d'une méthode qui intègre également un plan opérationnel des actions à mener en cas d'incident. Les organisations devraient appliquer des mesures de préparation internes et externes en mettant notamment en place un solide programme de formation des employés, des protocoles de communication et une équipe de gestion des menaces afin de prévenir les incidents tout en garantissant l'instauration de processus en cas d'incident.

Les données au cœur de l'approche

Comme nous l'avons constaté, le spectre global des défis et des sujets de préoccupation concernant la résilience opérationnelle est très vaste, mais une chose est sûre : les données constituent l'élément central du problème. Indispensables au fonctionnement des entreprises modernes, les données sont la cible des pirates derrière les ransomwares et d'autres cybercriminels menant des actes de malveillance. En protégeant vos données, vous serez en bonne voie pour protéger votre entreprise.

Un élément essentiel de la protection des données repose sur une architecture de résilience multiniveau efficace qui intègre une reprise des données multicouche exploitant les snapshots de sécurité afin de bénéficier de délais de récupération optimaux basés sur les besoins et les délais de récupération (RTO) de l'organisation. Si la capacité de récupération des données est cruciale, la récupération peut prendre plusieurs minutes, heures, jours ou un délai plus long encore et ne pas répondre aux exigences de l'entreprise, de vos clients ou des autorités de réglementation. En réalité, les autorités de réglementation et les institutions financières peuvent classer certaines charges de travail comme étant de « niveau 1 » et exiger ainsi leur récupération avec une interruption de l'activité minimale et une perte de données très limitée. En cas d'incident, qu'il s'agisse d'une catastrophe naturelle, d'une cyberattaque ou même d'un incident administratif, la vitesse de réaction et une capacité de récupération quasi instantanée sont déterminantes.

Bien que les snapshots de données soient un élément essentiel du plan, il est important de noter qu'ils ne sont pas tous créés de manière égalitaire. Les snapshots immuables ne peuvent pas être modifiés et pourtant, avec les privilèges appropriés, ils peuvent être supprimés. Une architecture véritablement résiliente repose sur des snapshots impossibles à modifier ou à supprimer, que ce soit par accident ou de manière intentionnelle (par une personne travaillant dans l'organisation ou à l'extérieur) pour offrir un point de récupération garanti. Pour bénéficier d'une « immuabilité supérieure », ces snapshots doivent être hors bande et soumis à une authentification multifacteur.

Les différents niveaux d'une architecture de résilience

Une architecture de résilience multiniveau est basée sur plusieurs niveaux ou couches de défense qui ont des objectifs spécifiques, uniques et importants. Ces niveaux contribuent à favoriser la vitesse et la durabilité de la stratégie de récupération.

Niveau 0

Ce niveau inclut (mais sans s'y limiter) une infrastructure stratégique (Active Directory, DNS ou services relatifs aux délais de réponse, par exemple). Sans ces services, aucun élément ou très peu d'éléments de l'environnement ne fonctionneraient.

Niveau 1

Les données primaires et les applications stratégiques pour vos opérations commerciales, y compris les principaux services d'application et bases de données, ainsi que leurs dépendances définies seront hébergées dans cette couche de résilience. Lors d'un incident, une organisation doit débuter la récupération le plus vite possible après l'incident, donc ces éléments seront l'objectif prioritaire de la récupération. S'ils sont indisponibles, votre organisation ne pourra pas offrir de services commerciaux à ses clients. Le niveau 1 devrait abriter trois à sept jours de snapshots véritablement immuables.

Niveau 2

Le second niveau fait office de niveau de réponse aux incidents. Les organisations peuvent s'en servir pour l'analyse des causes, la réponse aux incidents et la capacité de restauration élargie. Cette couche sert de copie d'archive pour le stockage des snapshots déchargés depuis le niveau 1. L'archive devrait pouvoir stocker des snapshots à moyen et long terme (au moins trois à douze mois ou plus longtemps si possible) et permettre aux équipes chargées de la réponse aux incidents d'obtenir immédiatement (et facilement) une vue à plus long terme de tous les incidents.

NOTE: *si le niveau 2 sert à stocker des données sur le long terme ou à répondre aux besoins en matière de conformité des données en cas de perturbation importante, cette couche peut également exécuter des charges de travail avec des performances légèrement réduites pour maintenir la continuité des opérations de l'entreprise.*

Niveau 3

Généralement, ce troisième niveau sert de couche de sauvegarde garantissant la rétention des données à long terme pour des besoins de conformité ou les données historiques, ou à restaurer des données pour des applications moins stratégiques qui ne nécessitent pas de protection des snapshots. Les organisations peuvent également utiliser ce niveau pour la sauvegarde en cas de scénario extrême.

Niveau 4

Le niveau 4 offre une couche de défense facultative (mais très fortement recommandée) constituée d'un bunker de données unidirectionnel en cas de sinistres de grande ampleur. Dans cette couche, les organisations peuvent répliquer leurs données sur un site totalement distinct. Les bunkers de données sont conçus pour être hautement sécurisés afin d'offrir une couche supplémentaire de durabilité. Ils peuvent en outre assurer le stockage crucial de plusieurs années de données, une condition requise par certaines autorités de réglementation. En cas d'incident, ce niveau permet aussi aux organisations de mettre en service des capacités de calcul à la demande de manière dynamique pour favoriser un retour rapide à un niveau opérationnel sans avoir à transférer des données sur de longues distances.

Encadré : résilience opérationnelle, cyberrésilience et continuité des opérations

La **continuité des opérations** et la **résilience opérationnelle** sont deux approches stratégiques, mais uniques de la gestion des risques. Bien que ces deux approches servent à faire face aux interruptions des opérations normales d'une entreprise, elles ont fondamentalement des points de départ opposés et se concentrent sur différents aspects de la réponse d'une organisation aux interruptions.

Même si la continuité des opérations et la résilience opérationnelle sont différentes, elles sont complémentaires et interconnectées. La continuité des opérations est une composante de la résilience opérationnelle, cette dernière intégrant davantage d'aspects tels que la gestion globale des risques, la **cyberrésilience**, la gestion des tiers et des crises. Ces deux approches sont stratégiques pour une organisation cherchant à assurer ses prestations de services dans des conditions difficiles.

La plus connue reste la continuité des opérations qui est principalement axée sur la récupération et la restauration de fonctions métier critiques après une interruption. Activé en cas d'incident, un plan de continuité des opérations est réactif par nature et son objectif principal est de limiter les interruptions, tout en accélérant le retour à la normale. La continuité des opérations repose généralement sur une approche coûts/bénéfices afin de déterminer la portée et l'échelle des activités.

En revanche, la résilience opérationnelle est un concept plus proactif et élargi qui inclut non seulement la capacité de reprise après des interruptions, mais aussi la capacité à éviter ou prévenir ces interruptions dans la mesure du possible. Contrairement à l'approche coûts/bénéfices de la continuité des opérations, la résilience opérationnelle est basée sur le postulat que le pire scénario va probablement se produire. La résilience opérationnelle implique non seulement la capacité à faire face aux interruptions et à s'y adapter rapidement afin de préserver la continuité de prestation des services essentiels, mais va bien au-delà de la récupération en incluant l'identification des vulnérabilités potentielles, l'atténuation des risques et l'adaptation aux changements de l'environnement opérationnel.

Du point de vue de cette conversation, la cyberrésilience est la seule préoccupation majeure. La cyberrésilience désigne la capacité d'une entité à fournir des services en permanence en cas de cyberattaques. À la différence de la cybersécurité conçue pour protéger les systèmes, les réseaux et les données contre les cyberattaques, la cyberrésilience permet de s'assurer que les systèmes et réseaux ne sont pas totalement inopérationnels en cas de compromission de la sécurité. Face à l'augmentation des attaques et leur sophistication croissante, la cyberrésilience apporte une réponse logique au fait que ce n'est qu'une question de temps avant qu'une attaque touche une organisation.

Comment les solutions Pure facilitent la résilience opérationnelle

Pure Storage propose des solutions parfaitement adaptées pour prendre en charge les besoins relatifs aux données de résilience opérationnelle des sociétés de services financiers. Bénéficiant d'une configuration 100 % flash qui maximise la vitesse et la flexibilité, ces solutions offrent une récupération et une sécurité des données intégrées optimales en cas d'interruption. Pure Storage s'assure de la prise en charge de la résilience opérationnelle dès la conception de ces solutions.

FlashBlade® et FlashArray™

Les solutions de données 100 % flash haute performance de Pure Storage sont parfaitement adaptées aux exigences accrues du secteur en termes de résilience opérationnelle. L'optimisation de la vitesse, de la simplicité et du débit renforce l'agilité de l'entreprise et lui permet de mieux respecter les accords de niveau de service (SLA) stricts en matière de protection et de disponibilité des données, qui sont essentiels pour garantir l'efficacité des opérations commerciales. Grâce à un portefeuille d'outils de stockage très homogène et basé sur une architecture commune (comprenant le logiciel Purity d'une grande fiabilité, des outils flash personnalisés et des outils de gestion partagés), l'utilisation peut être optimisée pour répondre aux exigences des charges de travail, avec des abonnements Evergreen™ qui permettent aux clients de faire face aux nouveaux défis et menaces sans interruption.

SafeMode

Pure offre également des fonctionnalités de protection des données performantes et intégrées avec SafeMode, qui assure la disponibilité permanente des snapshots de vos données. Basé sur la « règle des quatre yeux » selon laquelle seules deux personnes indépendantes et prédéfinies peuvent approuver des modifications, SafeMode protège les données et les métadonnées en créant des copies de snapshots sécurisées et immuables, impossibles à supprimer, à modifier ou à chiffrer même en disposant des identifiants d'un compte administrateur. Il s'agit d'un outil efficace, entièrement fonctionnel, flexible, automatisable et donc indispensable pour favoriser la résilience opérationnelle.

Restauration rapide

La résilience opérationnelle implique une reprise normale des opérations aussi rapide que possible. La fonctionnalité de restauration rapide intégrée à FlashBlade offre des capacités de récupération de l'ordre du pétaoctet afin de répondre aux exigences les plus élevées. Qui plus est, elle augmente considérablement la vitesse de restauration des données sans nécessiter le changement de votre logiciel de sauvegarde. Les systèmes hérités sont particulièrement lents et mal équipés pour les opérations de restauration et de récupération des données. Dans le même temps, l'architecture 100 % flash de FlashArray offre une sauvegarde et une restauration rapides permettant de dépasser les limites des architectures de protection des données héritées.

La résilience est au cœur de nos solutions

Architecture multiniveau sécurisée et évolutive avec Pure Storage, des partenaires de protection des données et d'autres contrôles et fonctions SIEM

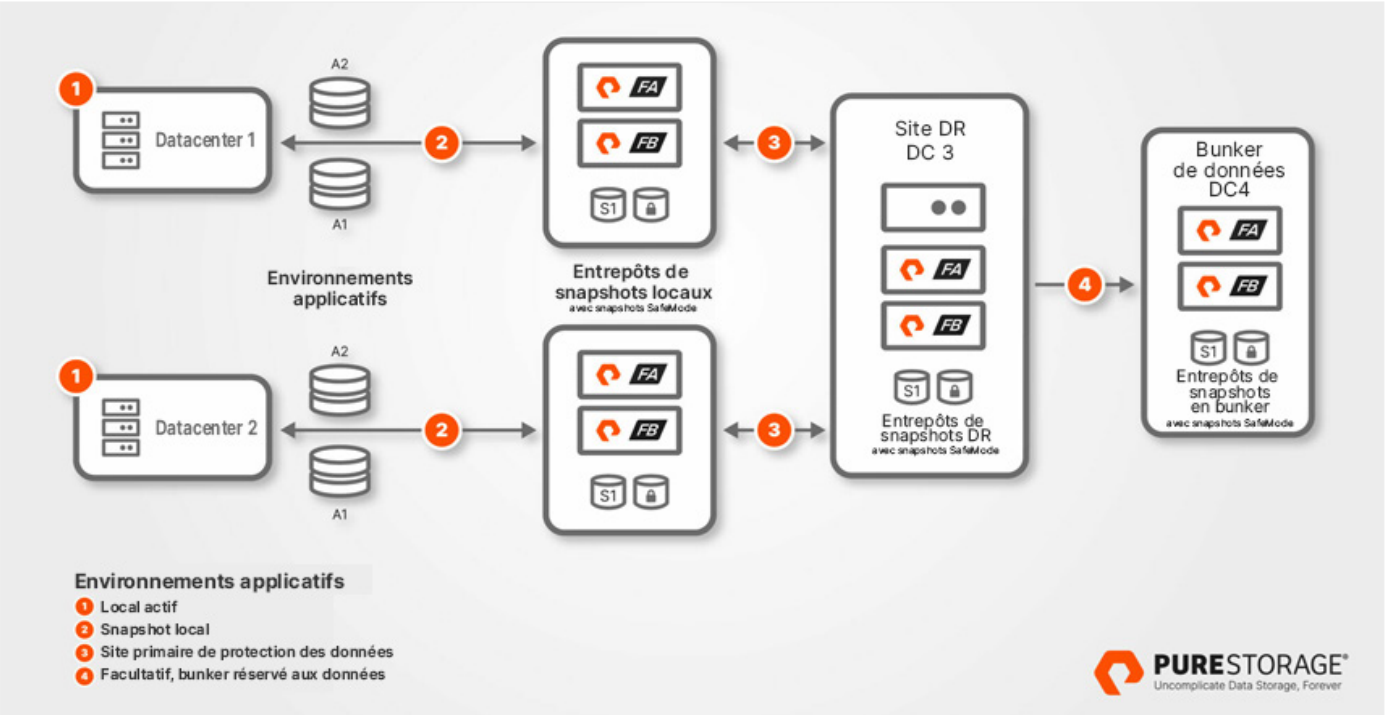

FIGURE 2 Fonctionnement d'une architecture de sauvegarde multiniveau

Autres fonctionnalités et capacités

- L'évaluation des systèmes et le support prédictif sont des processus simples avec Pure1®. Grâce à cet outil basé sur le cloud, vous bénéficiez d'une analytique complète avec un score de résilience des données et de la puissance pilotée par l'IA de Pure1 Meta® pour évaluer la vulnérabilité de votre environnement et vous permettre de remédier à ces faiblesses. Avec une interface unique pour gérer toutes vos baies de stockage, Pure1 offre une visibilité stratégique sur votre pile technologique, notamment une vue topologique pour faciliter la résolution des pannes sur les machines virtuelles.
- La solution Purity ActiveCluster économique et simple d'utilisation offre des niveaux de disponibilité exceptionnels. La solution à réplication synchrone active/active ActiveCluster garantit l'absence de points de récupération (RPO) avec un basculement transparent assurant des délais de récupération également nuls (RTO) entre des baies FlashArray.
- Pure Cloud Block Store™ offre un stockage en mode bloc cloud pour une mobilité des données parfaitement fluide sur les environnements on-premises et cloud, une protection des données cloud et des RTO et RPO rapides. Son chiffrement permanent et ses fonctionnalités de cybersécurité natives cloud en font une solution qui protège efficacement vos données, assure la conformité aux exigences réglementaires et sectorielles, préserve l'intégrité des données tout en garantissant une disponibilité permanente.
- Pure Protect //DRaaS est une solution de reprise après sinistre à la demande qui réduit la complexité, les coûts, les délais de récupération et les interruptions de service survenant à la suite de sinistres ou de perturbations liés à des cyberattaques. Grâce à cette solution, les entreprises disposent d'environnements sécurisés avec plusieurs points de restauration permettant de récupérer des copies sûres de leurs données vSphere on-premises sur des instances AWS EC2 natives, quelle que soit l'infrastructure de stockage sous-jacente, tout en assurant l'isolement des datacenters le temps d'enquêter sur l'incident qui les touche.
- Un SLA de reprise en cas d'attaque par ransomware pour une offre à la demande unique dans le secteur du stockage et une Garantie zéro perte de données sur le portefeuille Evergreen pour travailler en toute sérénité en évitant toute perte des données client en raison de problèmes liés au matériel ou aux logiciels de Pure Storage.

> « En cas de panne des systèmes, des milliards de dollars entrent en jeu et la réputation des entreprises est menacée. Nos clients ont besoin de services de données fiables et sécurisés. C'est exactement ce que Pure Storage garantit, en nous permettant d'établir des relations solides avec nos clients sur le long terme. »

JESSE BONSERIO, DIRECTEUR PRINCIPAL INGÉNIERIE, ABACUS GROUP[7]

Les solutions utilisant des supports flash sont idéales pour la résilience opérationnelle, car elles modifient radicalement la gestion de l'agilité des données dans les silos. Les performances et la fiabilité des supports flash offrent une nouvelle méthode de travail aux institutions financières qui peuvent l'exploiter pour améliorer la résilience opérationnelle de manière à relever les futurs défis de façon pertinente et à un coût concurrentiel, même pour les données froides.

Conclusion : renforcer la résilience opérationnelle des services financiers

La gestion des risques pour les services financiers évoluant en permanence, la résilience opérationnelle va devenir un élément incontournable des programmes de gestion des risques. Les autorités de réglementation internationales ont constaté que les marchés n'ont jamais été aussi interconnectés et que la technologie est le talon d'Achille[8] du système dans son ensemble. Avec l'adoption d'approches complètes comme la réglementation DORA, elles montrent qu'elles adaptent leur vision et leur gestion des risques. Les sociétés de services financiers doivent prendre conscience de ces enjeux et suivre leur exemple.

À l'instar du postulat de la résilience opérationnelle selon lequel des perturbations finissent par se produire, les institutions financières doivent également admettre qu'il n'est qu'une question de temps avant que les autorités de réglementation n'imposent des exigences plus élevées en matière de résilience opérationnelle. Parallèlement, les coûts liés à la non-conformité (amendes, autres coûts ou perte d'activité en raison de défaillances nuisant à la réputation de l'entreprise, par exemple) continueront également d'augmenter.

Les défis à relever sont considérables et la voie à suivre s'avère complexe et changeante, ce qui rend difficile l'élaboration d'un plan clair et efficace. Néanmoins, il est impossible d'ignorer le problème. Il ne faut plus attendre avant de se mettre à la tâche, même si cela implique d'avancer par petits pas au début. Au final, de grands changements surviendront, et les utilisateurs comme les processus devront s'y adapter. Il n'y a plus de temps à perdre.

Autres ressources

Étapes suivantes

- Découvrez ce qu'est une architecture de résilience et comment la créer.
- Découvrez comment les solutions de données Pure accélèrent les services financiers.
- Discutez avec un expert pour renforcer votre résilience opérationnelle.

Renseignements complémentaires

- Protection des données
- Continuité des opérations
- Atténuation des ransomware

À propos de l'auteur

Diane Saucier est directrice des services financiers de Pure Storage et dirige les initiatives de marketing pour les services financiers, les technologies financières et réglementaires. Diane a occupé des postes clés dans des institutions financières internationales et pour des fournisseurs de technologies. Ces fonctions lui ont permis de développer une stratégie de produits sur plusieurs classes d'actifs et des solutions de gestion du trading, des risques et de la conformité. Elle est l'un des membres fondateurs du Conseil d'administration de Women in Listed Derivatives (WILD) et membre consultatif du programme dédié aux fintechs à l'université de Floride du Sud et de la société John J. Lothian & Company, Inc. Diane est titulaire d'une licence en économie et en sciences politiques (Northwestern University) et détentrice d'un brevet pour un système flexible de commerce électronique.

1 As Risks Intensify, CEOs Can View Operational Resilience as a Competitive Advantage
2 BCBS Revisions to the Principles for the Sound Management of Operational Risk | PwC UK
3 UK Financial Regulators Levy Nearly £50 Million in Fines for Bank's Operational Resiliency Failures – Tech & Sourcing @ Morgan Lewis
4 Meeting the Challenge of HKMA Operational Resilience Requirements
5 PS21/3 Building operational resilience | FCA
6 Operational Resilience: It's a Global Issue
7 Abacus Group Builds Trust in the Finance Industry | Pure Storage
8 https://www.britishmuseum.org/blog/who-was-achilles

PS 2526-01-fr 02/24