Cyber-résilience

ÉTUDE DE SEPTEMBRE 2023

ANTICIPER ET GÉRER UNE CYBERCRISE

LES GRANDS THÈMAS

CIO.ÉTUDES

Cette étude a été réalisée et publiée à l'occasion
du Grand Théma « Cyber-résilience, préparer le jour d'après »,
organisé par CIO en septembre 2023.

La rédaction de CIO tient à remercier tous les répondants à
l'enquête qui ont ainsi permis la réalisation de cette étude.

Retrouvez les conférences CIO sur notre site web :
https://www.cio-online.com/conferences

Sommaire

Introduction

Pourquoi cette enquête ?

Les coûts liés à la cybercriminalité explosent dans les entreprises. Pour éviter de mettre en péril leurs activités, les entreprises doivent adopter une politique rigoureuse de gestion des risques et mettre en place la gouvernance et l'outillage nécessaire. Préparer les équipes et bien s'entourer figurent en tête de liste. Car, en cas de crise, l'humain sera toujours en première ligne. La résilience passe également par la mise en place d'architectures, de procédures et de contrôles robustes, un travail de fond à mener avec l'ensemble des équipes IT.

Du côté des solutions, les outils de sauvegarde/restauration demeurent incontournables pour se protéger face aux menaces de type ransomwares. Mais ceux-ci peuvent s'avérer complexes à mettre en œuvre dans des environnements de plus en plus hybrides et hétérogènes. Les solutions de réponse automatisée aux incidents peuvent également jouer un rôle précieux pour atténuer la charge des équipes de cybersécurité. Enfin, faut-il encore miser sur les cyber-assurances, dont le coût grimpe et les indemnisations diminuent ?

Dans le contexte de notre conférence Grand Théma « Cyber-résilience, préparer le jour d'après », CIO a voulu connaître la situation réelle dans les entreprises, en interrogeant les décideurs IT sur leurs pratiques.

Qui a répondu à l'enquête de CIO ?

La présente étude est basée sur une enquête réalisée en ligne du 5 juin 2023 au 15 septembre 2023.

De 180 à 250 entreprises y ont répondu (total variable selon les questions).

Se préparer à affronter une crise 1

Avez-vous une stratégie de sauvegarde en place pour les données essentielles de votre organisation ?

L'étude menée auprès de nos lecteurs montre que la majorité des organisations (56 %) ont une stratégie de sauvegarde pour leurs données essentielles. Cependant, il est préoccupant de constater que 35 % n'en aient pas encore, malgré l'importance de la protection des données critiques pour l'activité des entreprises et administrations, voire pour leur survie en cas de crise grave. Le potentiel d'amélioration est clair, avec 5 % en cours de mise en place d'une stratégie de sauvegarde et 4 % en réflexion.

56 % Oui

5 % En cours de mise en place

4 % En cours de réflexion

5 % J'aimerais bien

30 % Non

Vos sauvegardes font-elles l'objet de mesures de protection spécifiques (isolation, immuabilité ...) ?

Les résultats indiquent que 45 % des organisations prennent des mesures spécifiques pour protéger leurs sauvegardes, une mesure essentielle, car ces dernières sont une cible prisée des cybercriminels qui tentent de racketter les entreprises avec des rançongiciels. Cependant, il est préoccupant de constater que plus de 40 % des organisations (somme des réponses 'Non' et 'J'aimerais bien') ne prennent pas de telles mesures de protection. Les résultats mettent aussi en évidence la prise de conscience grandissante de l'importance de cet enjeu : 12 % des organisations ont lancé un projet ou réfléchissent à la protection de leurs sauvegardes. Il est également notable que 12 % des répondants aimeraient mettre en place de telles mesures, soulignant l'importance croissante de ce type de protection.

45 % Oui

6 % En cours de mise en place

6 % En cours de réflexion

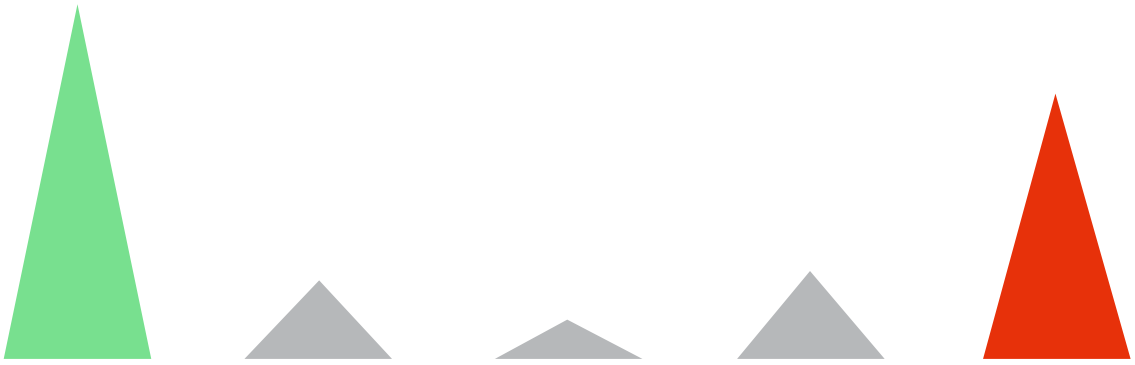
12 % J'aimerais bien

31 % Non

Se préparer à affronter une crise 1

Tous les éléments de vos infrastructures et systèmes critiques sont-ils redondés ?

Les résultats révèlent que 43 % des organisations ont déjà mis en place une forme de redondance pour tous les éléments de leurs infrastructures et systèmes critiques, démarche solide en matière de continuité. A l'autre bout du spectre, 44 % ne sont pas encore parvenus à assurer une couverture suffisante de leurs systèmes d'information critiques, malgré l'importance de cette mesure. Sur ce terrain, un potentiel d'amélioration existe, avec 9 % des répondants en cours de mise en place et 4 % en réflexion. Il est également notable que 10 % aimeraient mettre en place cette redondance, soulignant les inquiétudes croissantes relatives à la continuité d'activité des systèmes critiques dans l'esprit d'une part significative des répondants.



43 % Oui
9 % En cours de mise en place
4 % En cours de réflexion
10 % J'aimerais bien
34 % Non

Faites-vous des exercices de simulation de crise au sein de votre entreprise ?

32 % des entreprises réalisent déjà des exercices de simulation de crise, ce qui est considéré par les experts comme un facteur essentiel pour faire face aux imprévus, comme une attaque cyber paralysant les SI ou une panne informatique majeure. Cependant, il est préoccupant que plus d'une organisation sur deux ne se prépare pas à ces éventualités. L'importance de la préparation aux crises semble toutefois être bien comprise puisque 12 % des organisations sont en train de la mettre en place ou y réfléchissent. Il est également notable de constater que 11 % aimeraient effectuer de tels exercices, soulignant la reconnaissance croissante de ces derniers au sein de la communauté IT.

32 % Oui
6 % En cours de mise en place
6 % En cours de réflexion
11 % J'aimerais bien
45 % Non

Avez-vous souscrit une cyber-assurance ?

Seuls 18 % des entreprises interrogées ont souscrit une cyber-assurance. Malgré les risques croissants liés aux attaques cyber, plus de 8 entreprises et administrations françaises sur 10 n'ont donc pas souscrit d'assurance dédiée à ce stade. Les coûts de telles polices sont assurément un frein en la matière. 13 % des répondants indiquent toutefois que leur organisation est soit en train d'en mettre une en place, soit de l'étudier. Par ailleurs, 6 % des répondants aimeraient souscrire une cyber-assurance, suggérant une prise de conscience croissante de cet outil dans l'arsenal de protection des entreprises.

18 % Oui

7 % En cours de mise en place

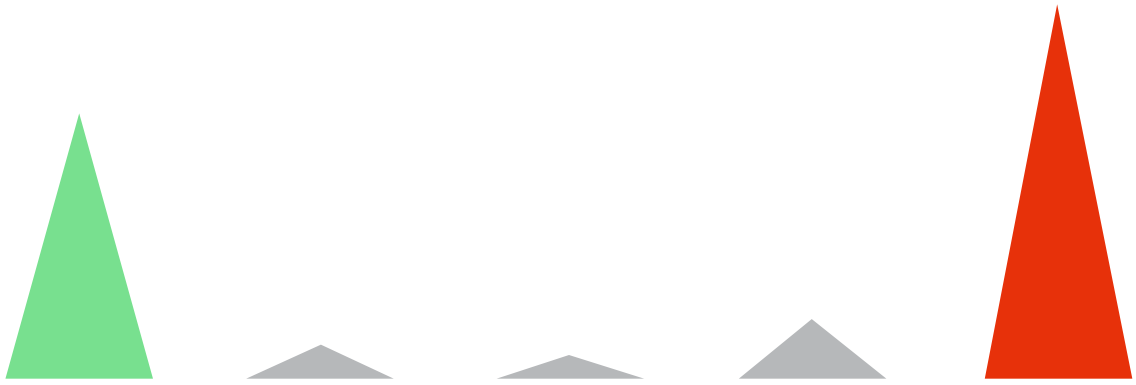
6 % En cours de réflexion

6 % J'aimerais bien

63 % Non

Disposez-vous d'une solution de monitoring sur vos opérations réseau et datacenters vous permettant de détecter rapidement les problèmes de performances ou des anomalies ?

Un tiers des entreprises dispose déjà d'une solution de monitoring pour leurs opérations réseau et datacenters, ce qui est positif pour la détection précoce des problèmes de performances et des anomalies. Cependant, il est préoccupant de constater que plus d'une organisation sur deux n'a pas encore mis en place de telles solutions, malgré leur importance pour maintenir la stabilité opérationnelle. D'ailleurs, dans ce pan du marché mal préparé, 11 % des répondants regrettent que leur entreprise n'ait pas avancé sur ce terrain. Comme dans la plupart des autres items de cette étude, une part significative des organisations – 11 % – a soit démarré un projet en matière de monitoring, soit à minima amorcé une réflexion.



33 % Oui

6 % En cours de mise en place

5 % En cours de réflexion

11 % J'aimerais bien

45 % Non

Avez-vous mis en place un système de gestion des informations et événements de sécurité (SIEM) pour être informé le plus en amont possible des menaces touchant votre SI ?

Environ une entreprise sur 4 a déjà mis en place un système de gestion des informations et événements de sécurité (SIEM) pour détecter les menaces en amont, ce qui indique un certain niveau de sensibilisation à la cybersécurité. Cependant, le sujet reste en friche dans plus de 60 % des organisations, ce que déplorent d'ailleurs 11 % des répondants. Là encore, le potentiel d'évolution est important, avec 7 % des organisations en cours de mise en place d'un SIEM et 8 % en réflexion.

24 % Oui

7 % En cours de mise en place

8 % En cours de réflexion

11 % J'aimerais bien

50 % Non

Gérer l'urgence 2

Disposez-vous en interne d'une équipe dédiée à la sécurité opérationnelle ?

37 % des entreprises et administrations disposent déjà d'une équipe dédiée à la sécurité opérationnelle, facteur positif en matière de protection des activités. Cependant, dans plus d'une organisation sur deux, une telle équipe n'est pas encore en place, malgré les enjeux croissants de sécurité. Là encore, la part des répondants qui aimeraient voir leur organisation progresser sur ce terrain est importante (12 %).
À l'inverse, les évolutions à court et moyen terme restent limitées, avec un faible 2 % des organisations en cours de mise en place d'une telle équipe dédiée et 4 % qui y réfléchissent.

37 % Oui

2 % En cours de mise en place

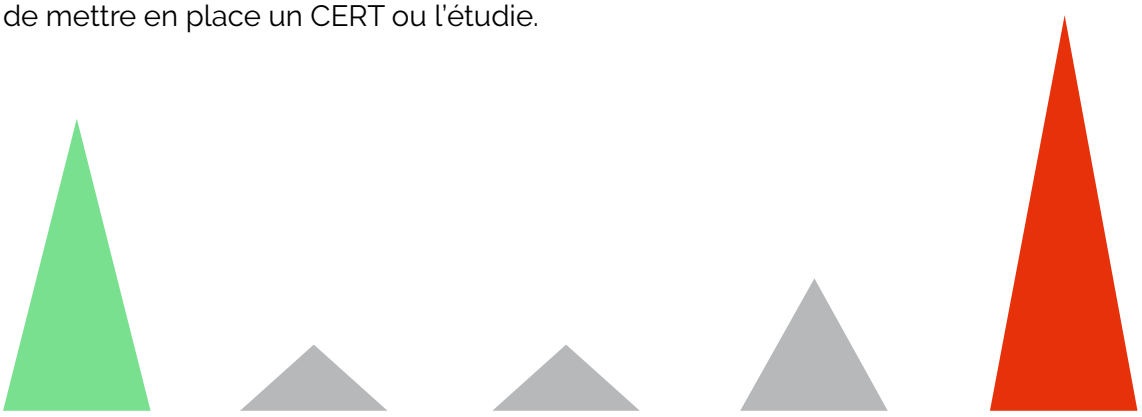
4 % En cours de réflexion

12 % J'aimerais bien

45 % Non

Pouvez-vous vous appuyer sur un CERT (centre d'alerte et de réaction aux attaques informatiques), qu'il soit interne ou externalisé ?

30 % des entreprises et administrations peuvent s'appuyer sur un CERT (centre d'alerte et de réaction aux attaques informatiques), outil clef pour détecter les attaques et y répondre. Encore souvent limité à des organisations de taille conséquente, le CERT reste hors de portée de plus d'une organisation sur deux, même si 13 % des répondants regrettent cet état de fait. Sur ce terrain, l'évolution du marché apparaît toutefois assez rapide, puisque 14 % des répondants indiquent que leur entreprise est en train de mettre en place un CERT ou l'étudie.



30 % Oui

7 % En cours de mise en place

7 % En cours de réflexion

13 % J'aimerais bien

43 % Non

Avez-vous un dispositif pour communiquer avec les collaborateurs en cas de coupure des systèmes et réseaux ?

Seule une entreprise ou administration sur trois a prévu un dispositif d'urgence pour communiquer avec ses collaborateurs en cas de coupure des systèmes et réseaux, ce qui est essentiel à la communication en situation de crise. À l'inverse, constater que près de 6 entreprises et administrations sur 10 n'aient pas encore un tel dispositif, malgré l'importance de cet aspect, est assez préoccupant. Notons qu'environ une organisation sur 10 est en train d'avancer sur ce terrain, via un projet déjà lancé ou une réflexion sur le sujet.

33 % Oui

4 % En cours de mise en place

5 % En cours de réflexion

7 % J'aimerais bien

51 % Non

Avez-vous prévu un mode de fonctionnement dégradé de l'entreprise, lui permettant de se passer de ses infrastructures critiques pendant une durée déterminée ?

De nouveau, on retrouve le ratio d'environ une entreprise et administration sur trois ayant bien anticipé une crise majeure, en prévoyant un mode de fonctionnement dégradé. Un facteur important de préparation à la continuité des activités. À l'inverse, malgré les risques, un tel plan n'est pas sur la table dans environ une organisation sur deux (ce que regrettent 8 % des répondants). Sur ce volet de la préparation de crise, l'évolution des mentalités semble assez rapide, puisque 5 % des organisations sont en train de déployer un mode de fonctionnement dégradé en cas d'indisponibilité de certains pans du SI et 10 % supplémentaires ont entamé une réflexion en la matière.

35 % Oui

5 % En cours de mise en place

10 % En cours de réflexion

8 % J'aimerais bien

42 % Non

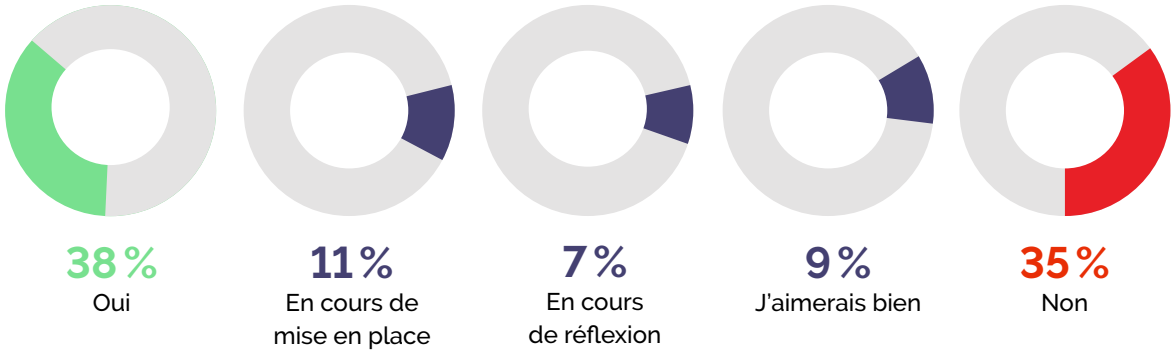
Rétablir les systèmes d'information 3

Testez-vous régulièrement la restauration des données ?

Pour s'assurer de l'efficacité des sauvegardes, tester régulièrement les opérations de restauration de données s'avère critique. Un aspect bien compris par 28 % des entreprises, qui mènent des tests réguliers. La précaution est toutefois ignorée par plus de 6 organisations sur 10, ce que regrettent d'ailleurs 12 % des répondants de la communauté IT, conscients de l'écart qui peut exister entre une garantie théorique et sa mise en pratique. Sur ce sujet, 5 % des organisations prévoient de déployer des tests de restauration de données à court terme et 5 % supplémentaires y réfléchissent.

Disposez-vous d'un plan de reprise d'activité (PRA) en cas d'incident ?

38 % des entreprises disposent déjà d'un plan de reprise d'activité (PRA), un outil essentiel de préparation aux incidents majeurs, quelle que soit leur origine. Cependant, il est préoccupant de constater que plus de 40 % n'en ont pas encore, ce que regrettent 9 % des répondants. Le sujet semble toutefois en évolution rapide, puisque 11 % des organisations sont en train de mettre en place un PRA et 7 % supplémentaires y réfléchissent. Gageons que la médiatisation de certaines attaques cyber et leurs conséquences pour les organisations touchées ont beaucoup fait pour faire évoluer les mentalités et débloquer les investissements correspondants.



Testez-vous votre PRA au moins une fois par an ?

Les experts du sujet expliquent que déployer un PRA sans le tester régulièrement revient à s'exposer à des déconvenues lors du déclenchement de ce plan. Les résultats de notre enquête montrent que seulement 28 % des entreprises testent leur plan de reprise d'activité (PRA) au moins une fois par an, 10 points de moins que la part des entreprises possédant ce type de mesures. Toutefois, 12 % supplémentaires sont en passe de mettre en place de tels tests ou l'étudient. Par ailleurs, l'importance des tests semble bien comprise dans la communauté IT, 15 % des répondants aimeraient que leur organisation teste son PRA au moins une fois par an, un niveau record sur cette enquête.

28 % Oui

5 % En cours de mise en place

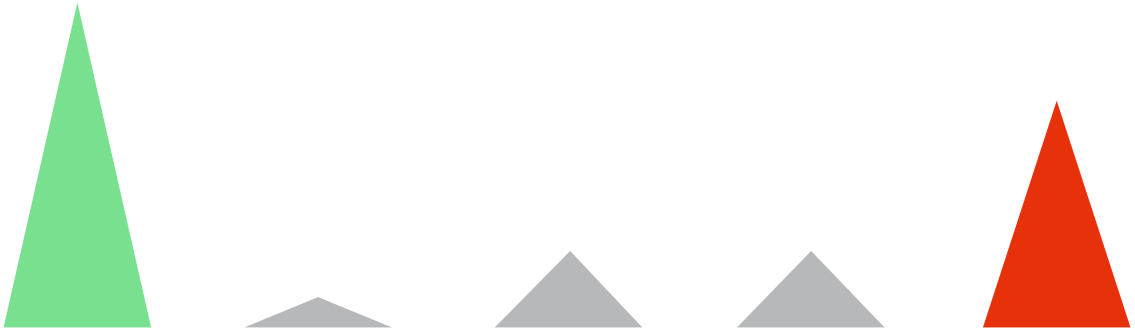
7 % En cours de réflexion

15 % J'aimerais bien

45 % Non

Lorsque votre SI connaît un incident sérieux, prévoyez-vous de façon systématique un retour d'expérience a posteriori pour en tirer des axes d'amélioration ?

Étant donné la complexité des systèmes et la sophistication des attaques, empêcher tout incident sur les SI relève du vœu pieux. Mais il est important de comprendre comme ces incidents se déroulent pour améliorer graduellement la résilience IT. 42 % des entreprises et administrations prévoient déjà systématiquement un retour d'expérience a posteriori (on parle aussi d'analyse post mortem) en cas d'incident sérieux. Mais, dans une part similaire d'entreprises et administrations, cette bonne pratique n'est pas systématique, ce que déplore d'ailleurs près d'un répondant sur quatre appartenant à cette catégorie. Sur ce terrain également, l'évolution du marché est assez rapide, 14 % des organisations étant en train de mettre en place ce type d'analyse ou y réfléchissant.



42 % Oui

4 % En cours de mise en place

10 % En cours de réflexion

10 % J'aimerais bien

34 % Non

Conclusion

Les résultats de notre enquête auprès des lecteurs de CIO révèlent un tableau contrasté du niveau de préparation des entreprises et des administrations françaises face aux crises de cybersécurité et aux pannes de sur leurs systèmes IT. Si certaines pratiques montrent une sensibilisation croissante aux défis de la sécurité informatique, d'autres indiquent un besoin urgent d'amélioration.

En ce qui concerne la gestion des données, il est positif de constater que la majorité (56 %) a mis en place une stratégie de sauvegarde, mais préoccupant de constater que 31 % ne l'ont pas encore fait. La protection des sauvegardes est également un domaine soulignant les limites des efforts de résilience des organisations françaises : seulement 45 % des entreprises prennent des mesures spécifiques pour les protéger alors que celles-ci sont des cibles prioritaires des cybercriminels.

Le constat est assez similaire en matière de préparation aux crises, avec des niveaux de préparation inégaux : seulement un tiers des organisations environ réalisent régulièrement des exercices de simulation de crise. La communication en cas de coupure des systèmes est essentielle, mais environ 6 organisations sur 10 n'ont pas encore de dispositif en place. Par ailleurs, une sur deux n'a pas prévu à ce stade un mode de fonctionnement dégradé de l'entreprise, lui permettant de se passer de ses infrastructures critiques pendant une durée déterminée.

Du côté de la surveillance des événements techniques en matière de production et de cybersécurité, on retrouve cette grosse majorité d'organisations qui ne disposent pas d'une solution de monitoring réseau et datacenter pour détecter rapidement les anomalies. Le constat est similaire si on s'attache à la présence d'une équipe chargée de la sécurité opérationnelle, à l'équipement avec système de gestion des informations et événements de sécurité (SIEM) ou à la surveillance par un CERT (Centre d'alerte et de réaction aux attaques informatiques).

L'étude permet aussi de mesurer l'évolution rapide des entreprises et administrations sur ces sujets, face à des risques cyber de plus en plus concrets et des conséquences opérationnelles de plus en plus massives. La part des organisations ayant lancé un projet ou réfléchissant au déploiement d'un PRA, d'un SIEM, à la mise en place d'un CERT ou d'un mode de fonctionnement dégradé permettant à l'entreprise de dépasser une crise atteint ou dépasse à chaque fois les 15 %. Par ailleurs, la proportion de répondants déplorant l'inertie de leur organisation sur des sujets comme les tests de PRA, les exercices de restauration de données ou la mise en place d'un CERT est, elle aussi, importante, soulignant la pression que mettent les décideurs IT sur leur organisation pour l'inciter à investir dans la cyber-résilience.

À propos de cio-online.com

CIO France est une plateforme multi-format de contenus et de services dédiée aux Directeurs de Systèmes d'Information (DSI ou CIO, Chief Information Officer) de grandes entreprises.

Les contenus et services en ligne, gratuits ou payants, sont associés aux événements tels que les Matinées Stratégiques.

CIO France est édité par IT News Info et est partenaire de CIO.com, un service du groupe IDG.

CIO www.cio-online.com

Contactez-nous

Pour toute information complémentaire :

Christelle Cadiou
Directrice Commerciale
+33(0) 1 81 51 71 31
ccadiou@it-news-info.com

Reynald Fléchaux
Rédacteur en chef
reynald.flechaux@it-news-info.com

Emmanuelle Delsol
Rédactrice en chef adjointe de CIO
edelsol@it-news-info.com

À propos de IT News Info

Grâce à son expérience acquise depuis 40 ans, IT News Info est le premier groupe d'information et de services pour les professionnels de l'informatique en France. Société éditrice de sites spécialisés sur l'actualité informatique, la transformation numérique des entreprises et l'innovation, IT News Info dispose également d'un Pôle Evénements, pour marier échanges d'expériences et création de nouvelles relations économiques, et d'un Pôle Marketing Services pour conjuguer communication à haute valeur ajoutée, génération de leads et bases de données qualifiées.
En 2007, IT News Info a fait le pari d'être le premier groupe de presse à basculer du print vers le web. Depuis, IT News Info ne cesse de développer de nouveaux services et d'innover pour conforter sa place de leader. IT News Info est une filiale des groupes IT Facto et IDG International.

IT NEWS INFO c'est :

CIO Distributique ENJEUX DAF ENJEUX LOGISTIQUES ENJEUX MARKETING ENJEUX RH

FRANCE ENTREPRISE DIGITAL LMI LEMONDE INFORMATIQUE LMI IT TOUR LEMONDE INFORMATIQUE RESEAUX TELECOMS