Livre Blanc du dirigeant

Anticiper la crise énergétique

20 recommandations pour la DSI

Version 1.1 du 3 novembre 2022

INFORTIVE
L'expert IT du Management de Transition

MAITRISE DES CRISES

infortive.com

maitrisedescrises.com

Table des matières

EXECUTIVE SUMMARY

Anticiper la crise énergétique pour la DSI

Une brusque coupure de courant peut avoir des effets désastreux sur nos Data Centers, les terminaux et les infrastructures informatiques, que ces dernières concernent les systèmes de gestion ou industriels.

La crise énergétique annoncée et la communication officielle des pouvoirs publics ne sauraient nous limiter à la mise en place de quelques mesures de bon sens. Elles nous incitent au contraire à anticiper et à mettre en place des plans d'action.

Les opérateurs électriques ont annoncé que la période dite de vigilance au niveau national a commencé dès le 1er octobre afin de pouvoir anticiper tout risque de difficultés ou de carence dans les approvisionnements en énergie électrique.

Concernant les systèmes d'information, le sujet est particulièrement critique, car les infrastructures informatiques générales du pays, du public ou du privé, sont de très gros consommateurs d'énergie, et tout arrêt non maîtrisé peut entraîner des dégâts considérables.

Prévoir une coupure partielle ou complète, faire en sorte que les activités critiques soient le moins impactées, maîtriser les redémarrages, accompagner les collaborateurs, s'assurer de la cohérence du plan énergie de nos fournisseurs avec le nôtre, comprendre les implications juridiques et assurance, prévoir un plan de communication si la crise est sévère… les points de vigilance sont nombreux.

Conscients de l'enjeu et de l'urgence d'une situation inédite qui se présente aux entreprises, Infortive et Maitrisedescrises.com se sont mobilisés afin de produire une seconde édition augmentée du présent guide visant à accélérer la préparation des entreprises face à une période incertaine.

Ce guide se veut pratique et opérationnel, afin de pouvoir éclairer rapidement les responsables dans les entreprises sur ce risque d'un format nouveau.

Il est évolutif et sera ouvert à la collaboration avec toute personne intéressée.

La démarche intellectuelle s'apparente à une opération de« déminage », visant à identifier les principales difficultés et les pistes d'actions permettant de les réduire.

Les scénarios de difficultés d'approvisionnement électrique

Les pouvoirs publics et les différents opérateurs électriques ont communiqué sur la façon dont pourraient survenir des difficultés dans l'approvisionnement électrique des entreprises. Le système de production et de distribution est basé sur l'équilibre entre l'offre et la demande. Les opérateurs ajustent la production en fonction de la demande, sous réserve de disposer de marges de manœuvre.

Cette année, compte tenu de l'état de disponibilité des outils de production d'électricité, notamment le parc nucléaire et les barrages de production hydroélectrique, **les opérateurs électriques ont mis en place un dispositif permettant de piloter la baisse de la demande dans l'hypothèse où la production serait insuffisante.**

Ce pilotage de la demande passe par plusieurs étapes progressives, dont l'appel à la sobriété pour les particuliers à travers l'application Ecowatt. Dans l'hypothèse où la demande serait trop forte, notamment suite à une météo très défavorable, une réduction de la consommation sera organisée auprès de certains industriels, d'appels renforcés à la population (Ecowatt rouge), avant si nécessaire d'envisager des délestages, c'est-à-dire des coupures sur des zones déterminées.

Si la situation le permet, on peut raisonnablement anticiper que ces délestages surviendraient plutôt dans des régions où la météorologie et la température seraient clémentes, afin de ne pas pénaliser d'autres régions de France qui rencontreraient au même moment des températures très froides. Cette forme de solidarité ferait reposer sur les entreprises installées dans des régions à météo clémente un risque plutôt supérieur de délestages. En revanche, en cas d'urgence, les délestages seraient organisés par les opérateurs de façon à protéger les installations de tout risque de surcharge ou d'endommagement. Dans la mesure du possible, les opérateurs informeront les particuliers et entreprises dans les zones concernées, **mais il faut aussi s'attendre à des manœuvres d'urgence** ne permettant pas un temps d'information suffisant pour protéger nos systèmes d'information.

Il est fortement recommandé de prendre connaissance des rapports et bulletins d'information officiels émis par RTE (https://www.rte-france.com/)

Bien entendu, les pouvoirs publics superviseront l'ensemble de ces manœuvres. Seront prioritaires : les opérateurs vitaux et essentiels, tels que les hôpitaux, les services de secours, les moyens de télécommunications, et bien entendu les datacenters et installations industrielles sensibles à la coupure si ces derniers sont connus ,identifiés et acceptés comme tels par les opérateurs.

Il convient donc de mettre en place un plan d'action visant à préparer l'entreprise à cette situation qui pourrait durer d'octobre à la sortie de l'hiver, et éventuellement se produire à nouveau les hivers suivants.

EN BREF

Nous rencontrons en France un risque d'approvisionnement d'énergie dû à un faible niveau des barrages et des centrales nucléaires en maintenance…

Nous devons trouver un équilibre entre production et consommation électrique

Si la météo est défavorable cet hiver, il faudra baisser notre consommation électrique

Des dispositifs seront mis en place pour baisser la consommation en urgence

- coupures gros consommateurs
- application Ecowatt
- délestages (coupures tournantes)

Nous devons mettre en place un plan d'action au sein des entreprises pour se préparer à cette situation, qui risque de devenir pérenne

1. Construire les plans d'action

Ces plans d'action doivent répondre à un double objectif :

Un premier objectif de sobriété, qui revient à participer à l'effort national de réduction de la consommation sur injonction des pouvoirs publics, c'est-à-dire de réduire, voire couper, l'ensemble des systèmes consommateurs non critiques pour l'entreprise.

Un second objectif de protection de l'intérêt des entreprises vis-à-vis des coupures et délestages, c'est-à-dire la mise en place de gestes d'urgence sur les activités informatiques et techniques critiques visant à les mettre en sécurité et permettre un redémarrage rapide dès que la situation le permettra.

EN BREF

Répondre à un double objectif : l'un, de sobriété énergétique et l'autre de protection de l'intérêt des entreprises.

2. Regrouper les ressources par niveau de risque

L'objectif de cette action est de conforter la classification des activités informatiques et techniques de l'entreprise en deux grandes catégories :

- la protection des activités et systèmes qui peuvent être éventuellement coupés sans compromettre le fonctionnement des activités vitales de l'entreprise,
- la protection des intérêts économiques et de la trésorerie, du climat social, et des activités de services industriels qui doivent être maintenus prioritairement en service.

Que faire ?

Il convient donc de lancer une opération de vérification et de regroupement des systèmes par classe de priorité.

Elle permettra d'identifier les activités critiques et non critiques et de les regrouper sur des machines physiques homogènes. Ces dernières pourront ainsi être coupées sans entraîner des activités informatiques virtualisées non homogènes en termes de criticité.

Cette opération permettra d'obtenir des groupes de systèmes homogènes pouvant être interrompus en cas de demande de sobriété de la part des pouvoirs publics. Il sera ainsi possible, si nécessaire, de couper de manière sécurisée les activités critiques dans l'objectif de les remettre en service le plus tôt possible dès que la situation le permettra.

EN BREF

Identifier les activités prioritaires pour les protéger

Pouvoir couper et remettre en marche de manière sécurisée les activités critiques

3. Baisser la consommation et participer à “l’effort de guerre”

L’objectif ici est de répondre à une alerte Ecowatt orange et rouge, c’est-à-dire une recommandation forte des pouvoirs publics demandant aux particuliers et aux entreprises de baisser la consommation.

Ecowatt contiendra des recommandations pratiques pour les particuliers, mais il appartient aux dirigeants des entreprises et notamment au Directeur des Systèmes d’Information d’en déduire les gestes techniques permettant d’atteindre cet objectif.

Que faire ?

Donner des consignes de bon sens aux utilisateurs, que ces derniers soient sur site ou en situation de télétravail : limitation du nombre d’écrans, coupure des appareils en dehors des périodes d’utilisation, réduire le volume des impressions, … On recommandera également de conserver les portables chargés afin d’être en mesure de travailler et d’être joignable en cas de crise.

Organiser la planification des opérations non critiques en dehors des périodes énergétiquement tendues, formaliser les procédures d’extinction et de coupure des activités non critiques, à la fois sur les Data Center, les postes de travail, les infrastructures, et l’ensemble des systèmes de climatisation, dans l’objectif d’un redémarrage dès que la situation le permettra.

Ces procédures formalisées devront recueillir un accord consensuel de la part des métiers, l’objectif n’étant pas d’entraver l’entreprise à ce niveau d’alerte mais simplement de couper tous les consommateurs dont l’activité peut être reportée telle que les études et développement, les machines de tests ou de recettes, etc.

EN BREF

Maîtriser les gestes techniques pour baisser la consommation d’électricité

Formaliser les procédures d’extinction

Valider les procédures avec les métiers

4. Couper partiellement

Une difficulté importante peut survenir lors des manœuvres de coupure partielle et de réduction des activités informatiques car la frontière entre des activités critiques et non critiques n'est pas toujours évidente. **L'objectif est de couper proprement ce qui n'est pas critique** en minimisant les effets d'interface non souhaitables vis-à-vis des activités critiques.

Que faire?

Analyser l'impact de tels phénomènes sur les infrastructures avec les différents responsables connaissant le mieux à la fois les infrastructures physiques des data Centers et des systèmes, et les architectes applicatifs notamment ceux des activités critiques.

Des ajustements pourront être effectués dans les procédures d'arrêt des systèmes non critiques, verrouillage des bases de données, fermeture des passerelles, fermeture des accès à des Web services extérieurs, etc.

EN BREF

Couper les activités non critiques sans répercussions sur les critiques

Analyser l'impact avec les responsables infrastructures physiques Data Centers et les architectes applicatifs

Ajuster toutes les procédures d'arrêt

5. Redémarrer en sécurité les activités non critiques

L'objectif est de maîtriser le redémarrage des activités non critiques mais également de permettre aux utilisateurs de prononcer en confiance un Go/NoGo une fois le redémarrage effectué. Ceux-ci doivent pouvoir se positionner sur la validité et la fraîcheur des données.

Que faire ?

Formaliser les procédures de redémarrage, c'est-à-dire organiser un redémarrage des applications dans un certain ordre et relancer les API/ interfaces batch qui n'auraient pas tourné.

Si il s'agit d'un arrêt général des serveurs, il faut mettre en place une méta-procédure de redémarrage ordonné.

Etablir une check list Go/ No Go sur la qualité des données, leur intégrité, leur niveau de sécurité afin d'informer les différents Métiers et leur permettre de reprendre leurs activités.

Anticiper l'ensemble des ces gestes pour toujours conserver des marges de sécurité.

EN BREF

Formaliser les procédures de redémarrage

Etablir une check list Go/No Go sur la qualité des données et leur niveau de sécurité

6. Vérifier les onduleurs

L'objectif est de maîtriser et de connaître l'autonomie des onduleurs, équipements qui possèdent des capacités de filtrage du courant afin de :

- le rendre de bonne qualité d'une part,
- pouvoir disposer d'une réserve d'énergie en cas de coupure de très courte durée, le plus souvent de l'ordre de la dizaine de minutes, d'autre part.

Ce délai est incompatible avec les délestages de deux heures qui ont été annoncés par les pouvoirs publics.

Que faire?

Engager très rapidement une action permettant de connaître l'autonomie effective des batteries vis-à-vis des activités maintenues en service et une action de réduction de la puissance consommée en aval afin d'augmenter le temps d'autonomie.

Délester très rapidement l'activité des systèmes non critiques augmente l'autonomie apparente des batteries des onduleurs. Dans certains cas on doit pouvoir arriver à la doubler, ce qui n'est pas négligeable, pour exécuter les manœuvres d'arrêt d'urgence si nécessaire.

EN BREF

Maîtriser l'autonomie des onduleurs

Connaître leur autonomie et réduire la puissance consommée pour la prolonger

Délester rapidement l'activité des systèmes non critiques

7. Maîtriser l'autonomie et l'activité des groupes électrogènes

L'objectif est de maîtriser l'autonomie et l'activité des générateurs électriques ou groupes électrogènes. Cette activité repose sur leur bon état, leur démarrage automatique en cas de coupure, et leur fonctionnement prolongé pour autant que leur puissance le permette, et que du carburant soit disponible afin de les alimenter tout au long des crises successives.

Que faire ?

Evaluer rapidement l'autonomie en temps des Data Centers :

- **En configuration nominale, c'est-à-dire « tout en marche »,**
- **En configuration réduite**, c'est-à-dire le non critique coupé, ainsi que leur système de climatisation..

En général, cette autonomie est de l'ordre d'un à quatre jours, ce qui permet d'encaisser plusieurs délestages successifs sur une même zone.

En déduire l'autonomie totale disponible des systèmes d'information critiques laissés en service derrière des générateurs, auxquels on retranchera le temps d'arrêt de ces mêmes systèmes critiques afin de sécuriser un arrêt « propre ».

Connaître et documenter les conditions de réapprovisionnement de carburant auprès de plusieurs fournisseurs, étant entendu que si la situation devait être critique au plan national, de très nombreuses entreprises et activités notamment publiques (hôpitaux, etc.) seraient prioritaires dans le réapprovisionnement en carburant. Il faut donc être lucide sur la réalité d'une réalimentation en carburant lors d'une situation tendue qui n'est pas individuelle à l'entreprise mais régionale, et d'agir si nécessaire auprès des services de la préfecture qui arbitreront les priorités dans de telles situations.

EN BREF

Évaluer l'autonomie des Data Centers en configuration "tout en marche" et réduite

En déduire l'autonomie des Systèmes d'Information critiques pour sécuriser un arrêt propre

Prévoir les conditions de réapprovisionnement de carburant

Certaines structures publiques seront prioritaires

8. Préparer une coupure propre et maîtriser les temps d'arrêt

L'objectif est de maîtriser la manœuvre d'un arrêt propre des Systèmes d'Information critiques, à l'intérieur de l'enveloppe d'alimentation électrique (réseau + onduleurs + groupe).

Que faire ?

Analyser la configuration applicative des activités critiques de l'entreprise et les procédures qui permettent d'intervenir dans l'ordre sur les systèmes. L'objectif est d'obtenir un arrêt sécurisé des systèmes et l'estimation des délais de coupure.

Au-delà du délai, l'ordre de redémarrage a aussi son importance et on les intégrera dans les procédures.

Réaliser un arrêt sécurisé dépend de l'état ponctuel des configurations systèmes, de la charge sur les machines physiques imposées par les serveurs virtuels regroupés par tranche de criticité, des volumes de données en transit dans les processus, des goulets d'étranglement éventuels sur les configurations, etc.

Le délai de "coupure propre" des systèmes critiques devra donc être noté dans les procédures d'arrêt des applications alimentées par des groupes. L'autonomie des groupes doit permettre d'aller jusqu'au bout des procédures d'arrêt en cas de carence d'approvisionnement en carburant.

La sécurité des systèmes, des biens et des personnes doit également être intégrée dans les procédures car couper et redémarrer des systèmes, c'est introduire en nombre des brèches de sécurité : sécurité au niveau des systèmes permettant des accès frauduleux non détectés, sécurité au niveau des personnels pouvant disposer de droits accrus de façon temporaire. On pourrait avoir beaucoup de mal à détecter une intrusion qui aurait lieu pendant un arrêt/redémarrage.

EN BREF

Analyser la configuration applicative des activités critiques pour intervenir dans l'ordre sur les systèmes

Noter le délai de "coupure propre" des systèmes critiques dans les procédures d'arrêt

Prévoir l'ordre de redémarrage des applicatifs

Intégrer la notion de sécurité et ne pas créer de failles pendant les opérations de coupures et reprises

9. Maîtriser le redémarrage des activités critiques

L'objectif est de parvenir à un redémarrage des activités critiques après un incident, et de pouvoir donner un Go/No Go au regard de la qualité des données et de la stabilité des systèmes en général.

Que faire ?

Formaliser les procédures de redémarrage, de remise en sécurité de l'approvisionnement électrique (batterie et réapprovisionnement en carburant), des systèmes de sécurité d'accès, des sauvegardes.

Chaque responsable de machine complexe (système d'information, machine industrielle, équipements de sécurité et gestion des bâtiments, etc... devra donc préparer une check list de vérification, procéder aux vérifications et envoyer un Go/ No Go à la cellule de coordination.

Permettre aux Métiers d'indiquer un Go / No Go clair basé sur la disponibilité et la fraîcheur des données en s'appuyant sur une gouvernance prédéfinie (Codir, DSI, comité adhoc)

Prévoir des systèmes de communication rapides et efficaces avec la cellule de crise pour gérer les redémarrages.

EN BREF

Formaliser les procédures de redémarrage

Prévoir des systèmes de communication redondants avec les métiers

10. Sécuriser les infrastructures de télécommunications et de télétravail

L'objectif est de maintenir en condition opérationnelle les infrastructures télécoms, dont celles participant au télétravail. Cette problématique repose sur les infrastructures (VPN, équipements de sécurité, alimentation des PC) quand ils sont au domicile de collaborateurs eux-mêmes délestés.

Par ailleurs, les infrastructures générales des opérateurs télécom (dont les opérateurs de téléphonie mobile répartis sur le territoire) sont en général alimentées par les installations des immeubles sur lesquels ils sont physiquement posés ou installés, et disposent de batteries de capacité limitée. Ils seront délestés au même titre que ces immeubles. il convient donc de prendre en compte des difficultés de communication (système, télétravail, joignabilité des équipes pendant les temps de coupure ainsi qu'une fragilité élevée pendant le temps de recharge des batteries.

Que faire?

Analyser la configuration d'alimentation en énergie des infrastructures côté serveur (dont les accès VPN) et en établir un profil de consommation ainsi qu'un impact sur l'autonomie générale du Système d'Information.

Anticiper les délestages importants dans des zones touchant les domiciles des collaborateurs effectuant des opérations critiques (trésorerie, équipe de gestion de crise, opérations informatiques, sécurité, communication, ressources humaines). Si nécessaire, équiper les collaborateurs de moyens de continuité électrique (onduleurs individuels) ou leur donner des recommandations qui peuvent aller jusqu'au déplacement en cas de situation d'urgence vers une zone non touchée.

EN BREF

Maintenir opérationnelles les infrastructures de télétravail

Établir un profil de consommation des infrastructures

En déduire son impact sur l'autonomie générale des Systèmes d'Information

Protéger les systèmes des collaborateurs effectuant des opérations critiques

11. S'assurer de la préparation de vos sous-traitants

Les activités informatiques des entreprises reposent sur un niveau de sous-traitance souvent élevé, qu'il s'agisse d'équipements ou de services près des infrastructures physiques (hébergement, cloud, Web services, sécurité managée, etc.), et ce, quelle que soit la taille de l'entreprise. L'objectif est donc de s'assurer que ces activités confiées à des fournisseurs font l'objet, au même titre que vos activités, d'un plan énergie visant à préparer à la fois la sobriété et les délestages éventuels.

Que faire ?

S'assurer que les sous-traitants critiques ont pu préparer leur propre plan fondé sur les mêmes priorités en les sollicitant formellement via un courrier en recommandé avec AR si nécessaire.

Il est utile de leur demander de partager leur plan dans la mesure où, la zone de vigilance annoncée par les opérateurs a commencé le 1er octobre 2022.

On pourra, dans un souci d'efficacité, guider et aider les fournisseurs critiques à très faible effectif qui n'ont pas nécessairement les moyens de concevoir un plan d'énergie. Le présent document peut leur être transmis afin de les guider.

EN BREF

S'assurer que le plan énergie de vos fournisseurs est basé sur les mêmes priorités que les vôtres

Demander de partager le plan énergie

Accompagner les fournisseurs critiques

12. Vérifier le bon fonctionnement des systèmes de cyber-sécurité et de sauvegarde

Le fonctionnement des systèmes de sauvegarde en cas de mise en œuvre des procédures d'arrêt sur les systèmes critiques est particulièrement essentiel à la mise en sécurité de l'entreprise et de ses données.

Par ailleurs, il est raisonnable d'anticiper une augmentation significative de la malveillance informatique (augmentation de phishing opportunistes exploitant la moindre non-vigilance des utilisateurs, attaques ciblées d'organisation étatiques ou non étatiques dans un contexte géopolitique instable....

Que faire?

Vérifier la bonne opérationnalité des systèmes de sauvegarde, leur configuration vis-à-vis des systèmes critiques et non critiques.

Vérifier le temps nécessaire à effectuer ces mêmes sauvegardes et leur mise en sécurité en cas de défaillance au redémarrage des systèmes dédiés à cette tâche.

En effet, il n'est pas rare lors du redémarrage d'un Système d'Information d'observer de nombreux incidents pouvant toucher des équipements électriques, alimentation, passerelle et système d'infrastructures, télécommunications, serveurs, disques, sauvegardes.

Dans le cas d'une coupure des systèmes critiques, la sauvegarde est le maillon ultime de la sécurité de l'entreprise, et doit donc être examinée de manière particulièrement attentive.

Renforcer et publier les recommandations sur la vigilance Cyber auprès des utilisateurs.

S'informer très régulièrement de l'état de la menace et des vulnérabilités auprès d'organismes officiels (Cer-ANSSI) et professionnels du secteur.

Enfin, on pourra éviter d'effectuer des mises à jour (notamment les BIOS) pendant les périodes Ecowatt rouge afin de limiter les risques de destruction du matériel.

EN BREF

Vérifier les systèmes de sauvegarde : temps, mise en sécurité des systèmes

Les incidents de démarrage sont fréquents

13. Anticiper des risques juridiques

En cas de situation tendue (températures très basses sur une large zone, un parc de production électrique indisponible, une solidarité européenne réduite dûe à une pénurie d'énergie globale), le nombre d'entreprises susceptibles d'être touchées défavorablement par les délestages pourrait être important entraînant ainsi **un risque systémique**.

Les difficultés des différents acteurs économiques peuvent avoir des conséquences financières en aval : impossibilité de produire, indisponibilité des données, perte d'exploitation, etc. Il est donc essentiel de bien préparer l'ensemble des entreprises et de l'économie pour limiter les **risques de recours en responsabilité** en cas de catastrophe en chaîne.

Par ailleurs, le risque de difficultés ayant été largement annoncé par les pouvoirs publics, le cas de force majeure ne pourra être invoqué. La responsabilité des entreprises non préparées pourra alors être engagée.

Que faire?

Contacter formellement les sous-traitants notamment les plus importants qui ont les moyens de préparer un plan de protection, et de le communiquer à leurs clients. Au-delà de tous recours, la prévenance des sous-traitants comprend une dimension informative et pédagogique.

Communiquer le présent guide à vos fournisseurs.

EN BREF

Limiter les recours en responsabilité

Encourager les sous-traitants à mettre en place un plan de communication et à le partager avec leurs clients

14. Assurance et responsabilité

En cas de difficultés importantes et de dégâts économiques et financiers significatifs liés à des interruptions d'activité d'un fournisseur en amont, ou de votre interruption impactant vos clients, des recours en responsabilité civile professionnelle.

Dans la mesure où les pouvoirs publics ont lancé et vont accroître leur effort de communication et de mise en alerte de l'ensemble des entreprises, il deviendra très hasardeux de pouvoir faire fonctionner le cas de force majeure en cas de difficultés systémiques.

En effet, pour que le **cas de force majeure** puisse être invoqué, l'événement doit être irrépressible, extérieur et imprévisible. Il ne sera pas facile de démontrer, après des mois d'alerte des pouvoirs publics, qu'une coupure électrique sur un Data Center n'était pas prévisible.

Les responsabilités en cascade peuvent amener les assureurs à examiner toutes les voies de droit permettant de limiter leur couverture en responsabilité civile.

Que faire ?

Examiner sans attendre, en impliquant les services juridiques des entreprises, les clauses contractuelles :

- Entre les différents intervenants dans la production informatique (sous-traitants, hébergement, service, etc.).
- Les clauses des contrats d'assurance de responsabilité civile qui vous couvrent, ou des contrats d'assurance de vos sous-traitants.
- Les clauses de hardship (clause de renégociation lorsque la survenance d'un événement de nature économique ou technologique, bouleverse gravement l'équilibre des prestations prévues au contrat).

EN BREF

En cas d'interruption impactant les clients, les voies juridiques seront examinées

Les assureurs prendront en compte que les pouvoirs publics ont anticipé l'alerte

Il faut rapidement examiner les clauses contractuelles et éventuellement prévoir des clauses de «hardship»

15. Audit

Dans le cas d'activité particulièrement critique comprenant des enjeux extrêmement élevés touchant des modèles économiques des entreprises, **il sera légitime d'inclure dans les plans d'audit fournisseurs la thématique de la protection contre les coupures électriques**. De telles demandes ont déjà été lancées, notamment entre les grandes entreprises et leurs fournisseurs informatiques, et vont naturellement se multiplier.

Que faire ?

En amont, interroger les fournisseurs critiques au moyen de grilles d'audit rapides. Celles-ci vous permettront de vous assurer de l'engagement de ces mêmes fournisseurs dans la mise en place de moyens de protection et de préparation.

En aval, préparer des éléments de communication factuels concernant votre propre préparation de façon à rassurer vos clients.

EN BREF

Intégrer la protection contre les coupures électriques dans les plans d'audit fournisseurs

16. Communiquer en amont auprès des fournisseurs

Au-delà des questions de responsabilité, en cas de situation nationale particulièrement tendue, il faudra communiquer en amont afin d'informer les principaux sous-traitants contribuant à vos activités critiques de l'éventuelle interruption de vos activités, et d'avoir connaissance de toute interruption effective de leurs activités ayant un impact chez vous.

Que faire?

Établir un plan de communication fournisseurs visant à fluidifier les informations d'interruption dans les deux sens et incluant les procédures d'urgence consécutives à une alerte Ecowatt concernant l'une des deux parties.

EN BREF

Fluidifier la communication avec les fournisseurs incluant les procédures d'urgence

17. Communiquer en interne auprès des collaborateurs, impliquer les Ressources Humaines

La mise en place par les pouvoirs publics d'un canal d'information et d'alerte visant à piloter la baisse de la consommation électrique repose sur l'outil Ecowatt. Celui-ci permet de cibler les particuliers en leur donnant des recommandations de sobriété souhaitable ou urgente afin de prévenir les délestages et les coupures.

Les collaborateurs des différentes entreprises vont y être sensibilisés et mettront en œuvre des mesures de sobriété énergétique à titre personnel.

Ces mêmes collaborateurs attendront de l'entreprise qui les emploie un comportement cohérent, voire exemplaire, en termes de sobriété. Cette réaction est aussi probable dans les entreprises que chez les sous-traitants ou les clients.

D'autre part, en cas de délestage par grand froid, les immeubles non secourus ne seront plus chauffés si ventilés, les blocs de secours indiquant les issues de secours, les systèmes de sécurités alimentés par des batteries à capacité limitée seront hors service.

Dans ce cas, les locaux devront être évacués pour des raisons de sécurité. En cas de températures basses dans les locaux ou de remise en question de la sécurité, le droit de retrait pourra être invoqué.

Que faire ?

Impliquer la Direction des Ressources Humaines (DRH) sur les questions de sécurité au travail, la possibilité d'exercice du droit de retrait en fonction des dispositifs de continuité électrique (groupe électrogène...). Les instances représentatives du personnel devront être informées de la nature du plan. En particulier le plan de vérification de la bonne opérationnalité des systèmes de sécurité (blocs de secours, télésurveillance, alarmes...) pourra être porté à la connaissance des IRP dans un objectif de préservation de la confinace.

Concevoir et mettre en place un plan de communication en cas d'alerte Ecowatt visant à prolonger dans l'entreprise les recommandations qui seront données aux particuliers.

Les Systèmes d'Information jouent un rôle essentiel dans ce plan car ils sont responsables de structures fortement consommatrices d'électricité.

Ce plan de communication doit donc être préparé, validé par la DSI dans l'objectif de maintenir un niveau d'adhésion des collaborateurs de l'entreprise le plus élevé possible.

EN BREF

Les collaborateurs vont être personnellement encouragés à moins consommer d'énergie

Ils attendront un comportement exemplaire de l'entreprise

Communiquer auprès d'eux sur votre engagement et les mesures prises

Valider ce plan de com côté DSI et en parallèle avec la DG/DRH et DIR COM...

18. Communication d'urgence

En cas d'urgence, l'entreprise pourra être amenée à réduire, voire couper des activités importantes supportées par les systèmes d'information, et même des activités critiques. Il convient bien entendu d'en informer les équipes sans délai, les coupures pouvant intervenir très brutalement.

Que faire ?

Établir un plan de communication d'urgence visant à informer les collaborateurs des indisponibilités des systèmes, de leurs éventuelles conséquences et des voies pour les contourner.

Placer un annuaire des personnes à joindre dans un endroit (physique ou virtuel) accessible quelque soit les circonstances.

En particulier dans le cas de l'interruption des outils de communication (messagerie, outils collaboratifs, système d'alerte, téléphonie, etc.), les informations devront être transmises vers les collaborateurs concernés sans délai en leur indiquant comment maintenir un niveau minimum de communication avec le management.

EN BREF

Organiser une communication d'urgence :

- Pouvoir prévenir les équipes sans délai des indisponibilités du système

19. Conduire des opérations gestion de crise

En cas de situation particulièrement tendue et prolongée, l'entreprise sera très sérieusement perturbée par des délestages ou menaces de délestages répétitifs dans l'ensemble de la chaîne de valeur dans lequel elle opère.

Dans les prévisions les plus défavorables, les opérateurs électriques ont annoncé qu'une trentaine de situations d'urgence pourraient être déclenchées entre octobre et la fin de la période froide.

Il est donc légitime de préparer le fonctionnement d'une cellule de crise visant à piloter ces opérations.

Que faire ?

On pourra donc établir la liste des participants à une telle cellule de crise, en précisant les moyens de communication nécessaires et alternatifs. Dans des situations extrêmes, les membres de la cellule de crise pourront être amenés à se déplacer afin de pouvoir se positionner dans une zone normalement alimentée en énergie et en télécom afin de retrouver les moyens d'agir.

EN BREF

Organiser une cellule de crise :

- liste des participants
- moyens de communication alternatifs
- repli vers une zone alimentée en énergie

20. Préparer la fragilité électrique dans le temps

À l'heure où sont écrites ces lignes, il est difficile d'anticiper les conditions météorologiques et de température qui prévaudront sur l'ensemble du territoire. Il est possible à ce stade que les entreprises aient à faire face à des opérations répétées visant à préparer l'entreprise, informer les collaborateurs, répéter les gestes techniques les plus critiques, délimiter les différents périmètres, sécuriser les données, mettre en œuvre des opérations de réduction de la consommation voire de coupure totale, redémarrer les systèmes, communiquer avec les sous-traitants et clients, sécuriser le volet juridique.

Ces différentes manœuvres dans un tel contexte sont très largement inédites. Il existe donc une courbe d'apprentissage significative devant nous.

Que faire ?

Anticiper et préparer l'amélioration de la qualité de l'ensemble du dispositif en alimentant une main courante et un enregistrement de l'ensemble des opérations, des succès et bien entendu des échecs, de réaliser des points d'étape à la fin de chaque grande action (notamment des redémarrages importants) et de mettre en place un système d'amélioration de la performance de l'ensemble du dispositif.

En particulier, le présent guide de bonnes pratiques publié par Infortive et maîtrise-descrises.com a pour objectif et vocation de s'améliorer dans le temps et sera ouvert à la collaboration avec toute personne intéressée. Vous pouvez envoyer vos propositions de collaboration à aduportal@infortive.com.

EN BREF

Ces inputs sont une façon de nous préparer à la crise

Nous allons apprendre en marchant et mettre en place des RETEX pour améliorer nos dispositifs

Vous pouvez contribuer à améliorer ce guide en nous envoyant vos propositions

Présentation des auteurs

Maitrisedescrises.com

Maitrise-des-crises.com fournit aux dirigeants et leurs collaborateurs directs des éléments d'analyse et de recommandations concernant l'ensemble des risques systémiques majeurs pouvant affecter le fonctionnement des entreprises. Présenté sous un format très largement audiovisuel, il permet d'informer, d'alerter et de guider les dirigeants en temps réel très en amont de la survenance de risques systémiques tels la pandémie, le contexte international, la cyber sécurité, les catastrophes naturelles et le changement climatique, et bien entendu la crise énergétique. Maîtrisedescrises.com est animé par Vincent Balouet, qui fut dès 1992 le premier français à l'origine de la mobilisation nationale pour la résolution du bogue de l'an 2000 dans les entreprises, auteur des principales publications d'abord au CLUSIF, puis appelé en urgence au CIGREF afin de mettre en place le dispositif pour les grandes entreprises et produire l'essentiel des publications, puis mobilisé par le MEDEF et enfin par BERCY afin de guider et baliser la trajectoire pour les PME et la cellule de crise du gouvernement. C'est la même démarche aujourd'hui qui préside à la réalisation de ce guide : celle de l'anticipation et du déminage.

Infortive Transition, un cabinet de Management de Transition au positionnement novateur

Infortive Transition a été créée par des DSI de Transition, persuadés que les Systèmes d'Information sont au cœur de la stratégie de l'entreprise.

Infortive Transition propose aux entreprises des managers de transition pour accélérer leur transformation digitale, mener des projets de transformation, gérer des crises, assurer un intérim au pied levé…

Présentation des auteurs

Les dirigeants d'Infortive, anciens DSI de transition, s'appuient sur leur expérience de terrain pour sélectionner les meilleurs managers et les accompagner tout au long de la mission. Ils sont garants de leur maîtrise technologique et de leur capacité à mener l'accompagnement de projet.

Infortive anime la première communauté de DSI/CTO de transition en France qui apporte une intelligence collective et répond aux besoins de progrès et d'échanges de ses membres.

La Communauté des DSI de transition Infortive

Première communauté de DSI de transition en France, Infortive réunit des professionnels de la Direction des Systèmes d'Information entraînés par leurs missions de transformation aux situations d'urgence.

Les recommandations publiées dans ce guide sont une illustration de leur capacité à intervenir rapidement et en mode collaboratif.

Ils mettent leurs compétences aux services des entreprises qui doivent gérer des transformations : fusion d'entreprises, carve out, externalisation des infrastructures, déploiement d'un projet international, rationalisation des coûts, transformation digitale.