LES DOSSIERS TECHNIQUES

Cyberénergie :

Comprendre et se préparer aux répercutions d'une crise énergétique sur la sécurité et la résilience de vos activités

Janvier 2023

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Jean-Marc	**BOURSAT**	TotalEnergies

Les contributeurs :

Fabrice	**POLLART**	Maisons et cités
Olivier	**STASSI**	Bpifrance
Patrick	**ARMUSIEAUX**	iMSA
Alpha Bady	**BALDE**	France Télévisions
Delphine	**DE SAINT CYR**	Bourse Direct
Vincent	**GIORGI**	CPRPSNCF
Sandrine	**REDOUTE**	Devoteam
Vincent	**BALOUET**	Maitrisedescrises.com
Patrick	**CHAUVIN**	Autorité des Marchés Financiers
Eric	**EGEA**	NTT France

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

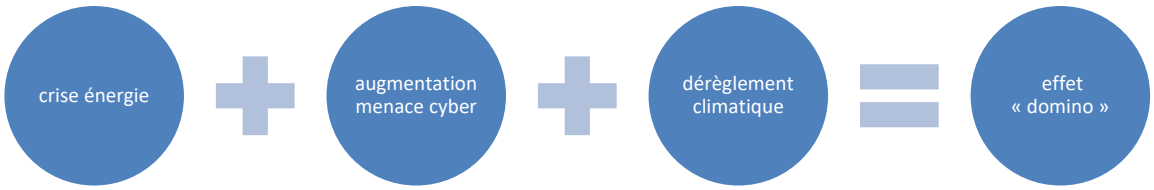
PARIS, 13 octobre 2022 (Reuters) - La France ne pourra pas éviter des délestages massifs d'électricité en cas d'hiver normalement froid ou très froid, a déclaré jeudi Philippe Page le Mérour, secrétaire du comité social d'entreprise central d'EDF, estimant que les capacités d'effacement ne suffiront pas.

« *La crise énergétique évoquée dans les médias provient du fait que la France pourrait ne pas être en mesure de s'approvisionner pour couvrir les pics de consommation cet hiver.*

L'Europe est actuellement touchée par une crise énergétique exceptionnelle. Il s'agit en premier lieu d'une crise gazière, apparue au second semestre 2021 avec des tensions sur l'offre et la demande d'énergie après la reprise économique mondiale post-Covid, puis amplifiée par la guerre menée par la Russie en Ukraine et la forte réduction des livraisons de gaz russe qui en a résulté.

…

Néanmoins, la situation particulière de l'année 2022 conduit à s'écarter de ce tableau pour ce qui concerne l'électricité. Depuis l'identification d'un défaut de corrosion sous contrainte sur certains réacteurs, une seconde crise, portant sur la production nucléaire, s'est ajoutée à la première crise sur le gaz. Cet été, la disponibilité du parc nucléaire a été en retrait de 15 GW par rapport à une situation nominale. À cela s'ajoute une sécheresse longue et intense, en France et dans une large partie de l'Europe, qui a également largement amoindri la production hydraulique. La situation en France est donc dégradée également sur la production d'électricité, conduisant le pays à importer davantage, et donc à dépendre plus directement du cours des énergies fossiles »[1]



Ces conditions particulières ont mené RTE à publier, dès le mois d'octobre 2022, le résultat de l'étude saisonnière pour informer le public et les acteurs économiques et leur permettre ainsi de s'organiser et d'anticiper d'éventuels délestages.

Dans ce contexte, le Clusif a souhaité comprendre les risques induits par cette crise et aider les décideurs à se préparer aux répercussions qu'elle pourrait avoir sur la sécurité et la résilience[2] des Systèmes d'Information.

[1] Basé sur le rapport RTE, Perspectives pour le système électrique pour l'automne et l'hiver 2022-2023 – résumé exécutif

[2] La résilience est la capacité de résister aux chocs. Ce terme est communément employé pour les matériaux et dans le domaine de la psychologie. Par analogie, cela s'applique au domaine IT dans le sens de la capacité à surmonter une crise IT.

L'objectif de ce document est en particulier de présenter les impacts potentiels sur :

- les opérations cyber (maintien en condition de sécurité) ;
- les équipes cyber, SOC, CERT,
- les collaborateurs,
- le niveau de menace cyber.

… et de proposer des conseils pour les réduire.

La prise de conscience doit permettre au management d'intégrer cette réalité dans leurs scénarios et de s'autoévaluer sur leur niveau de préparation à fonctionner en mode dégradé ou très dégradé sur une période plus ou moins longue.

1.1 Contexte IT

Une rupture d'approvisionnement électrique est un risque pris en compte dans les plans de continuité mais généralement avec un prisme sur les sites et les datacenters. Les équipes opérationnelles sont (ou devraient être) formées pour faire face à ce type d'incident. L'alerte de RTE modifie les hypothèses prises :

- les coupures seront a priori précédées d'alerte sur l'alimentation électrique – et par conséquent, il faut intégrer ces alertes dans le processus de prévention,
- les coupures peuvent être répétées et plus ou moins longues[3] – et il faut se préparer à répondre à plusieurs arrêts, ce qui complique la tâche,
- les coupures vont aussi impacter les employés – et il faut vérifier que les plans de continuité intègrent ce volet.

Le site monecowatt.fr fournit une carte météo de l'électricité avec trois niveaux de tension sur le système électrique et par conséquent d'alerte : vert, orange et rouge.[4]

Le niveau d'alerte Orange correspond à une surveillance renforcée des distributeurs d'énergies.

En cas d'alerte de niveau rouge sur une zone, celle-ci risque de subir une coupure de courant estimée à 2 heures maximum[3] (sauf surincident du réseau de distribution).

Il faut donc intégrer ce scénario de coupure d'énergie dans la liste des scénarios de déclenchement d'un PCA. Cela suppose que les sites de repli soient dans des zones de distribution électrique différentes du site impacté et que les moyens de secours électrique soient capables de tenir au moins deux heures.

Une rupture d'approvisionnement électrique aura un impact sur la communication au niveau professionnel et personnel. Cela peut impacter les réseaux mobiles, le fonctionnement des numéros d'urgence[5] et les accès Internet professionnels ou personnels. Il faut se préparer à une désorganisation au sein de son entreprise.

Une coupure non précédée par un arrêt propre des équipements peut les détériorer. Le fait de connaître à l'avance le risque de coupure doit permettre d'anticiper les opérations de mise hors tension des équipements les plus critiques et d'effectuer des sauvegardes afin d'être en capacité de restaurer sur du matériel de secours.

Pour éviter une rupture, tout le monde peut fournir des efforts de sobriété énergétique. La mesure de sa consommation et la définition d'actions de réduction de sa consommation ne sont pas des mesures cyber, mais il faut étudier les impacts cyber des actions : par exemple

---

[3] Deux heures maximum pour un arrêt programmé. C'est la durée communiquée par les autorités au moment de la rédaction de ce document

[4] Ecowatt | votre météo de l'électricité pour une consommation responsable (monecowatt.fr) Equivalent pour les alertes gaz : Ecogaz - Baromètre du gaz (myecogaz.com)

[5] Communication Orange Business Service du 13/12/2022 : « Le réseau mobile sera quant à lui inopérant 10 à 30 minutes après le début de la coupure électrique… »

éteindre un serveur par mesure d'économie, impacte la capacité à appliquer des correctifs de sécurité sur le serveur.

Les bonnes pratiques ont fait l'objet de publications, notamment par :

- le CIGREF

  (https ://www.cigref.fr/crise-energetique-contributions-des-directions-numeriques)

- Infortive

  (https ://www.infortive.com/actualites/anticiper-la-crise-energetique-20-recommandations-pour-la-dsi).

L'objet du présent document n'est pas de reprendre ou de compléter les propositions faites mais d'apporter un éclairage Cyber sur celles-ci.

1.2 Considérations cyber

La désorganisation plus ou moins importante d'une entreprise ou administration est souvent le moment choisi par les entités malveillantes pour tenter d'en tirer profit. Il faut donc s'attendre, en plus de la gestion des problèmes directement liés aux coupures électriques, à subir des tentatives d'hameçonnage, de désinformation, d'infections diverses ou d'intrusions avant, pendant ou après ces coupures électriques.

Ce phénomène peut être amplifié si le maintien en condition de sécurité (mises à jour, application des correctifs, …) n'a pas pu se faire dans des conditions normales durant les perturbations.

Il faut aussi prendre en compte le cas des collaborateurs qui se replient dans un lieu public (bar, restaurant, gare …) pour continuer à travailler. Ils doivent être sensibilisés à cette pratique et bénéficier de solutions de connexion sécurisée lors de l'utilisation de Wi-Fi public. Il faut aussi les sensibiliser aux comportements à adopter dans un lieu public en termes de gestion de la confidentialité afin d'éviter la fuite d'information. Dans tous les cas, les consignes de l'entreprise doivent être claires sur cet usage.

Les équipes cyber doivent se préparer à réagir à ces scénarios de crise énergétique et elles doivent accompagner les décideurs de leur périmètre de responsabilité avant, pendant ou après une période de coupures pour réduire le risque de sur-incident cyber.

Si un site sans alimentation électrique ne risque pas de subir une attaque logique, il faut vérifier que les infrastructures de secours sont aussi bien sécurisées que les infrastructures nominales. Il ne faut pas oublier que la désorganisation des équipes peut être un facteur aggravant dans la gestion de crise.

Il faut aussi prendre en compte les solutions Cloud utilisées pour la protection cyber de l'entreprise. Il est donc opportun de s'assurer que les fournisseurs de ces solutions aient bien eux-mêmes mené une démarche similaire afin de garantir l'innocuité de coupures électriques sur les services sécurité.

2 Impacts cyber d'une crise énergétique

Ce chapitre décrit les impacts cyber d'une crise énergétique en trois parties :

- sous l'angle technique, directement liés à l'IT,
- sous l'angle organisationnel,
- sous l'angle humain.

2.1 Impacts techniques

L'impact télécom est évident : sans électricité, il n'y a plus de réseau informatique ni de réseau téléphonique. L'impact cyber d'une coupure réseau ou plus globalement d'une coupure des moyens de communication doit être étudié en fonction du contexte de chaque organisation.

La bascule des utilisateurs sur le partage de connexion depuis un smartphone risque d'entrainer une saturation des antennes téléphoniques encore en activité et d'augmenter le nombre de *points d'accès* frauduleux. Il est d'ailleurs prévisible que les antennes relais téléphoniques soient également touchées par les mêmes coupures électriques et que leur secours électrique dure moins d'une demi-heure.

La Voix sur IP (*VoIP*) sera directement impactée et aucune communication ne sera possible durant la coupure, jusqu'à restauration du réseau informatique.

L'impact sur les infrastructures et les applications est amplifié par le nombre de composants potentiellement impactés. Il peut se concrétiser par un endommagement physique d'équipements qui auraient subits des coupures trop fréquentes. Il faut également prendre en compte les infrastructures mutualisées mises en œuvre par les propriétaires des immeubles. Ceux-ci risquent d'être débordés si des interventions manuelles sont nécessaires pour réinitialiser le réseau.

Au titre du maintien en condition opérationnelle, il faut vérifier que les moyens de secours électriques des petits ou moyens sites, onduleurs ou groupes électrogènes, sont bien opérationnels et les tester régulièrement. A priori, les *datacenters* de niveau *3* et 4 n'auront pas de problème et leurs engagements sur ce sujet font partis des contrats d'hébergement. Cependant la situation exceptionnelle peut être à l'origine de dysfonctionnements des moyens de pilotage de l'énergie d'un site et générer des arrêts partiels ou complets de *datacenter*. Dans ce cas, il est conseillé de vérifier les options de redondance choisies par les solutions SaaS et les hébergeurs.

D'un point de vue cyber, la perte d'une partie de son IT peut :

- perturber ou empêcher la connexion des utilisateurs au reste de l'IT non coupé (solution d'identification/authentification non opérationnelle),
- perturber ou supprimer les moyens de protection des applications (route de secours moins ou pas sécurisée),
- perturber les opérations de maintien en condition de sécurité (service de mise à disposition ou mise en œuvre des correctifs indisponible ou inaccessible),
- perturber ou interdire la détection d'incident cyber (impact sur les outils du SOC ou sur les communications de ces outils avec le reste de l'IT),
- perturber les opérations de réaction à un incident cyber (impact sur les équipes CERT et leur capacité à intervenir à distance).

La sécurité physique des sites peut également être impactée :

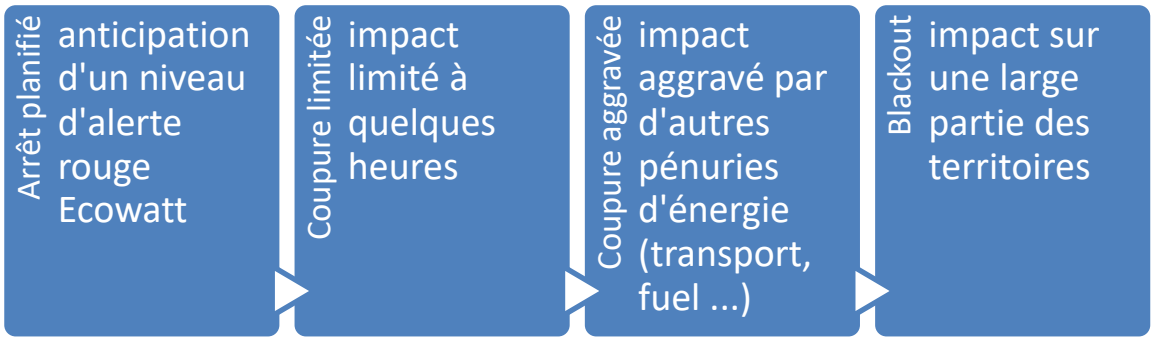
- une coupure de courant peut impacter les équipements de gestion des accès, les systèmes de badges, les portes équipées de serrure magnétique qui risquent de ne plus remplir leur rôle et par conséquent d'augmenter le risque d'intrusion physique,
- les systèmes de détection d'intrusion et les moyens de vidéo surveillance seront aussi impactés. Il faut donc vérifier les consignes données aux équipes de gardiennage.

2.2 Impacts organisationnels

Les impacts organisationnels sont amplifiés s'il n'y a pas d'équipe cyber dédiée. Dans la suite du paragraphe, le terme « équipe cyber » fait aussi référence aux équipes IT en charge des opérations cyber. Le manque de préparation en amont des équipes cyber engendre des risques de perte de capacité de protection, détection et réaction. Elles seront livrées à elles-mêmes pour gérer des problèmes inédits sans possibilité de communiquer ou d'accéder à de la documentation. La documentation de continuité d'activité doit intégrer les tâches à réaliser en cas de coupure électrique (à compléter si ce n'est pas le cas).

Dans le cas des arrêts planifiés, l'entreprise doit définir son plan de réaction face à un tel arrêt, et les équipes cyber doivent surtout contrôler que le plan d'action ne crée pas de nouveaux risques cyber. Les équipes cyber doivent aussi s'organiser avant, pendant et après l'arrêt pour anticiper et traiter les éventuels problèmes.

Il faut considérer les impacts des décisions qui peuvent être prises en situation de crise. Les entreprises doivent définir les responsabilités préalablement à la crise pour prendre certaines décisions comme celle d'arrêter un datacenter ou de basculer les utilisateurs sur un site de secours ou en télétravail généralisé par exemple. Il faut prendre en compte les niveaux d'impacts suivants :



Dans le cas des arrêts non planifiés, l'entreprise est normalement déjà préparée à traiter une coupure électrique d'un site ou d'un *datacenter*. Cependant la crise énergétique ne concerne pas uniquement l'électricité, mais aussi les énergies utilisées pour les groupes électrogènes (la répétition des coupures pourrait entrainer des difficultés à remplir des cuves de carburants[6] par exemple). Dans ce cas, les équipes cyber devraient être sollicitées selon la procédure de gestion d'incident habituelle. Il faut qu'elles soient préparées à intervenir en mode dégradé, avec un accès à l'énergie perturbé.

Si la crise énergétique s'amplifie, les dysfonctionnements dans les réseaux de transport ou la fourniture de carburants (pour les groupes électrogènes des *datacenters* par exemple) pourront aggraver la désorganisation[7].

L'impact organisationnel concerne aussi les fournisseurs, prestataires, sous-traitants qui peuvent être perturbés dans la fourniture de biens ou de services à l'entreprise. Il faut évaluer, si ce n'est pas déjà fait, la criticité des services ou des biens, et évaluer les fournisseurs critiques sur leurs mesures prises concernant la crise énergétique (sur les flux logistiques en particulier).

La gouvernance et la gestion de crise doivent être en place pour impliquer les équipes IT et cyber selon les cas.

---

[6] Il est recommandé de disposer d'un contrat d'approvisionnement intégrant une livraison prioritaire si l'on ne dispose pas d'une grosse capacité de stockage.

[7] Cas des onduleurs pour les sites utilisateurs

2.3 Impacts humains

L'impact humain est le plus important[8] : chacun risque d'être touché dans sa vie professionnelle et personnelle. La crise énergétique va impacter les transports, les communications, les écoles et les crèches, le chauffage dans les bâtiments, l'approvisionnement en biens et nourriture… autrement dit tous les aspects de nos vies qui nécessitent de l'énergie. Au pire, cela peut aussi impacter la vie ou la santé de la population si les établissements de santé ou de secours sont impactés – être coincé dans un ascenseur ou un métro ne sont pas des scénarios improbables.

D'un point de vue cyber, l'impact humain est plutôt indirect. Il ne faut pas perdre de vue que les collaborateurs n'auront pas nécessairement leur attention dirigée sur la sécurité de l'information et les bonnes pratiques de sécurité de leur entreprise. Les équipes cyber doivent prendre en compte le fait que la vigilance des collaborateurs sera amoindrie en temps de crise. Il faudra aussi prendre en compte le problème de la mise à jour de leur poste de travail. Pour les équipes cyber, le traitement des opérations cyber risque d'être impacté du fait de la réduction des équipes et d'éventuelles difficultés à communiquer.

En revanche les comportements des utilisateurs durant les coupures peuvent être dangereux, en particulier les messages échangés sur les réseaux sociaux. Il faut impérativement sensibiliser les utilisateurs aux comportements à éviter.

Les risques psychosociaux sont aussi à prendre en compte et les managers doivent être formés pour identifier ces risques et les traiter au cas par cas pour éviter des comportements qui pourraient entraîner des conséquences malheureuses en termes cyber.

[8] La protection des personnes est un devoir de tous.

3 Nos conseils pour réduire les impacts

L'objectif de ce paragraphe est d'amener l'organisation à se poser les bonnes questions et de proposer des pistes de réflexion si la question n'a pas été traitée au sein de son entreprise.

Avant de rentrer dans le détail, la crise énergétique renvoie à la crise COVID qui a démontré que la préparation aussi bien technique qu'organisationnelle est capitale pour limiter les impacts.

3.1 Conseil #1 : Communiquer

Ce chapitre porte sur le plan de communication à faire en amont car il sera compliqué de communiquer durant les périodes de coupures électriques.

☐ *Avez-vous communiqué sur le sujet de la crise énergétique auprès de votre management et de vos collaborateurs ?*

Si non, mettez en place un plan de communication interne en ajoutant les conséquences potentielles de la crise sur le volet cyber.

☐ *Avez-vous intégré les données d'Ecowatt dans votre intranet pour vos collaborateurs ?*

Si non, mettez-le dans l'intranet et définissez comment ces informations seront traitées par l'entreprise et transmises aux équipes concernées.

Vous pouvez également communiquer par mail sur la procédure à suivre pour consulter Ecowatt.

☐ *Avez-vous défini la communication en interne et en externe en cas d'alerte orange ou rouge Ecowatt ?*

Si non, définissez comment ces alertes seront traitées par l'entreprise et transmises aux équipes concernées.

Il faut également adapter les messages prévus dans le plan de crise.

☐ *Avez-vous défini une sensibilisation des utilisateurs spécifiquement liée à la crise énergétique ?*

Si non, définissez les messages de sensibilisation sur les bons ou mauvais réflexes à avoir en fonction des décisions prises par l'entreprise sur la gestion de la crise.

Il faut sensibiliser au risque de surincident possible par une augmentation des attaques dans un moment où l'entreprise est potentiellement désorganisée ou déstabilisée par les effets de la crise énergétique. Ces messages doivent être adaptés selon les cibles, des dirigeants jusqu'aux collaborateurs.

Il faut également sensibiliser les collaborateurs sur l'ingénierie sociale.

☐ *Avez-vous modifié les consignes de sécurité pour prendre en compte les scénarios spécifiques à la crise énergétique ?*

Si non, définissez les consignes de redéploiement du personnel et les consignes pour les visiteurs.

Parmi ces consignes, l'usage de solutions cloud alternatives au SI doit être encadré.

☐ *Avez-vous défini les messages à envoyer en cas de perturbations liées à la crise énergétique aux clients ou partenaires ?*

Si non, préparez un plan de communication d'urgence (messages avant, pendant – si possible et après).

3.2 Conseil #2 : Se préparer au pire

☐ *Avez-vous vérifié que l'entreprise ait bien anticipé les ruptures d'approvisionnement énergétique dans la durée (plusieurs occurrences durant plusieurs semaines) ?*

Si non, vérifiez s'il n'est pas prévu de réaliser de la maintenance préventive ou une réorganisation des opérations en fonction de l'évolution de la crise énergétique.

Il faut également s'assurer de la disposition de la documentation sous forme papier. En cas de coupure électrique, la documentation électronique sera indisponible.

☐ *Avez-vous défini des arbres de décisions spécifiques au traitement de la crise énergétique ?*

Si non, prévoyez des arbres de décisions (pour les arrêts planifiés et les arrêts non prévus) intégrant les considérations cyber.

En particulier, les arbres de décisions doivent tenir compte des délais d'interruption et les répétitions des événements. 2 heures de coupure ne nécessitent pas toujours une bascule en mode crise[9].

Il faut aussi s'assurer que les consignes données aux administrateurs (fiches réflexe) précisent bien les attendus en cas de coupure ou de rupture d'énergie :

- Que faire si je n'ai plus d'accès aux SI (total ou partiel) ?
- Que faire si je ne peux pas venir sur site ?
- Que faire si les opérations cyber sont perturbées ?

Ces arbres de décisions doivent être déclinés selon les différents scénarios (coupure planifiée, coupure exceptionnelle, coupures répétées, blackout).

☐ *Avez-vous défini une période de gel des opérations IT dès que le niveau d'alerte orange ou rouge est atteint ?*

Si non, prévoyez un gel des opérations pour limiter les impacts, surtout en cas de coupure non planifiée durant des opérations d'installation ou de changement majeur.

☐ *Avez-vous défini des consignes particulières si un administrateur ne peut pas assurer ses tâches car il est lui-même impacté par la crise énergétique ?*

Si non, vérifiez que la gestion des backups de personne est bien opérationnelle.

☐ *Avez-vous prévu d'augmenter ou mettre en place des équipes de gardiennage en cas d'indisponibilité des contrôles physiques ?*

Si non, étudiez une solution pour ajouter des gardiens en cas de besoin. Une analyse des risques liés aux intrusions physiques ou vols d'équipements devra être menée avec un plan d'actions associé.

☐ *Avez-vous défini des consignes particulières sur les mesures à prendre lorsque les serveurs éteints par mesure d'économie durant une période de plusieurs semaines sont rallumés ?*

Si non, vérifiez que l'application des correctifs de sécurité publiés durant la période est intégrée dans les consignes.

[9] Le délai de prévenance sera très court : Eco watt va surtout indiquer la potentialité d'une coupure. Sa réalité pour un site ne sera confirmée que vers 21h30 la veille sans garantie sur l'horaire de l'arrêt. Difficile dans ce contexte de prévenir le personnel.

☐ *Avez-vous défini un ou plusieurs responsables de la surveillance du niveau de crise Ecowatt ?*

Si non, vérifiez que le RPCA ou un équivalent a bien pris cette responsabilité, comme pour le sujet de crise liée à une crue centennale.

☐ *Avez-vous vérifié les clauses contractuelles de vos hébergeurs ou fournisseurs Cloud concernant l'approvisionnement électrique de vos ressources ?*

Si non, contrôlez si les engagements de vos fournisseurs sont conformes à vos attentes et si les options de redondances ont bien été souscrites pour les ressources ou applications critiques à vos activités.

☐ *Avez-vous évalué votre niveau de préparation ou capacité de résilience face aux coupures de courant ?*

Si non, anticipez d'éventuelles questions lorsque le niveau de la crise énergétique augmentera et que ce sujet sera au cœur de l'actualité nationale.

☐ *Avez-vous fait valider votre stratégie de prise en compte de la crise énergétique par votre direction ?*

Si non, faites le car les décisions difficiles à prendre ne doivent pas être découvertes par la direction durant la crise, au risque de ne pas intégrer la cybersécurité dans les choix.

Une validation de la stratégie permettra de réagir plus rapidement et efficacement. La communication vers la direction sera d'autant plus facilitée.

4 Glossaire

Acronyme / Terme	Signification	Plus d'explication
CERT	Computer Emergency Response Team	Centre d'alerte et de réaction aux attaques informatiques
CIGREF	Club Informatique des Grandes Entreprises Françaises	
COVID	CoronaVIrus Disease	Maladie à coronavirus
Datacenter		Centre hébergeant les équipements d'un Système d'Information
EcoWatt		Application et Plateforme en ligne créées par RTE pour informer les consommateurs d'électricité
EDF	Électricité De France (Entreprise)	
Impact		Conséquence d'un incident
INFORTIVE		Cabinet de Management de Transition IT
Correctif	Modification d'un logiciel système ou applicatif permettant de corriger une faille de sécurité	
Reuters	Agence de presse britannique	
RPCA	Responsable du Plan de Continuité d'Activité	
RTE	Réseau de Transport d'Électricité (Entreprise)	
SaaS	Software as a Service	Logiciel en tant que service
SOC	Security Operations Center	Division qui assure la sécurité du SI au sein d'une organisation
Niveau (Datacenter de)	Classification du niveau de disponibilité d'un datacenter	
VoIP	Voice over Internet Protocol	Transmission de la voix sur réseau IP
Wi-Fi	Wireless Fidelity	Réseau sans fil

Tour Eria
5 rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr