EVICYS

EXPERTS EN CYBERSÉCURITÉ

La nécessité d'une gouvernance cyber

Webinaire Tenerrdis - 05 décembre 2024

Votre interlocuteur

Raphaël Vignon-Davillier

Président et co-fondateur

Expert en cybersécurité, et officier de réserve Cyber, j'accompagne les entreprises d'Auvergne-Rhône-Alpes dans la protection de leurs systèmes d'information et la gestion des risques numériques notamment en tant que RSSI à temps partagé.

Je suis également actif au sein de réseaux professionnels régionaux en AURA.

EVICYS
EXPERTS EN CYBERSÉCURITÉ

Qui sommes-nous ?

Evicys est un cabinet de conseil en cybersécurité qui accompagne les TPE, PME et ETI de la région Auvergne-Rhône-Alpes.

Nous collaborons notamment avec des sociétés des secteurs de la médecine nucléaire, de l'industrie manufacturière, et de l’industrie des jeux et divertissement (casinos).

Notre mission est d’apporter une solution novatrice et abordable qui renforce la résilience des entreprises de la région Auvergne-Rhône-Alpes

Agilité

Budget adapté

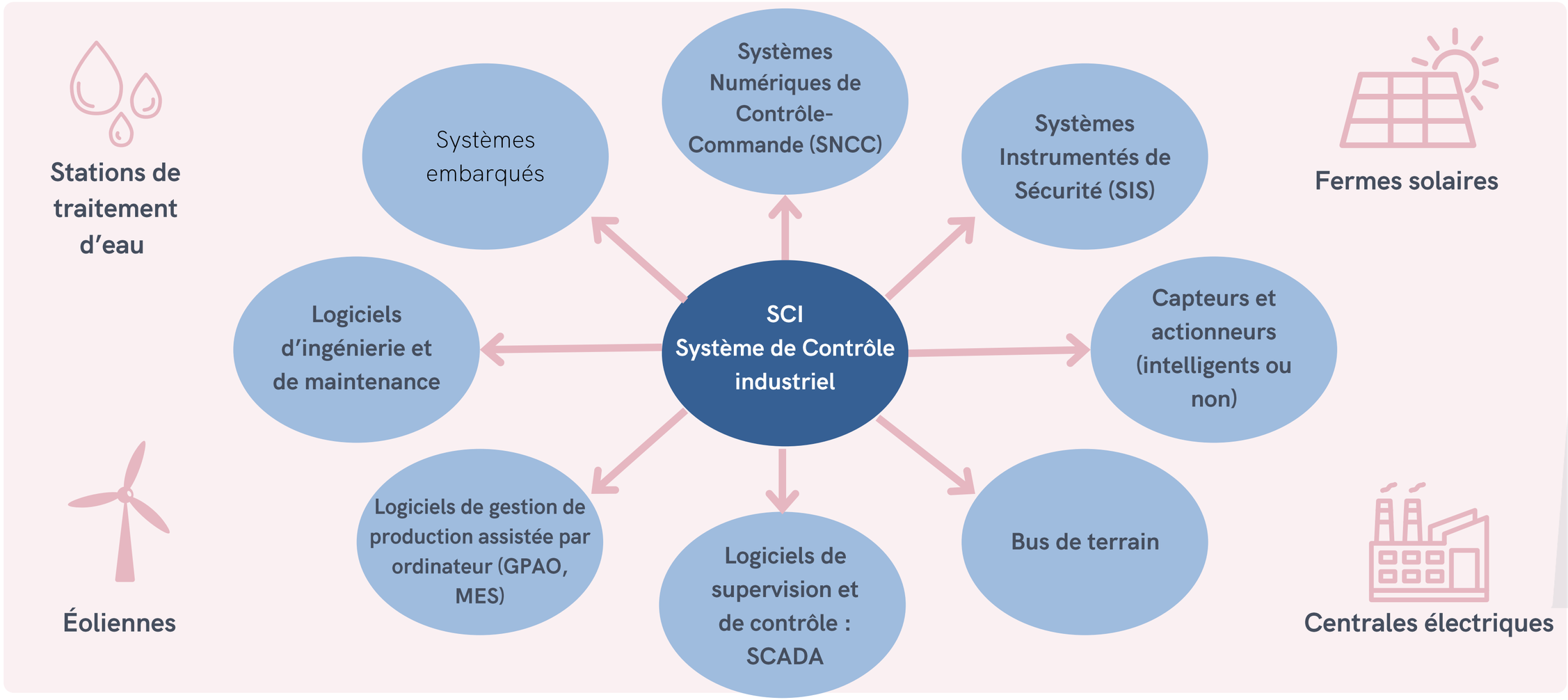
Proximité

EVICYS
EXPERTS EN CYBERSÉCURITÉ

La nécessité d’une gouvernance cyber

Contexte des systèmes de contrôle industriel

Les Systèmes de Contrôle Industriel (SCI) regroupent les systèmes destinés à la surveillance en temps réel et à la conduite centralisée d'équipements industriels distants ou locaux (moteurs, vannes, pompes, relais, etc.), d'équipements de sites tertiaires assimilés, ou la gestion globale de systèmes tels que les SMART GRID.



L’évolution de l’éco-système

Gouvernance Cyber

La transformation numérique et les nouveaux usages ▶ exposent les SCI aux menaces Cyber ▶ qui induisent de nouveaux risques ▶ aux conséquences catastrophiques

- accès distants (opérations maintenance)
- standardisation technologique IP windows, BDD
- large recours aux interconnexions

- surface d’attaque augmentée
- conformité réglementaire IEC 62443, NIS2
- espionnage industriel, déstabilisation
- hacktivisme

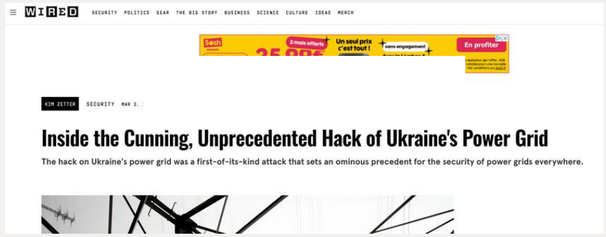
- mise en danger des personnels d’exploitation, des sous-traitants et des tiers
- perte de production ou interruption de service
- atteinte à l’environnement, à la santé du public
- perte d’équipements
- copie, vol, perte de données sensibles

- pertes humaines
- pertes financières
- perte de confiance
- perte de compétitivité
- condamnation, violation de lois ou réglements

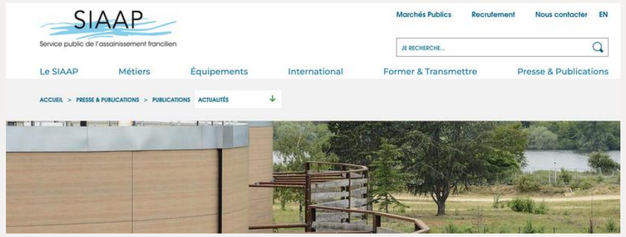
EVICYS
EXPERTS EN CYBERSÉCURITÉ

Quelques exemple d’incidents cyber dans l’industrie énergétique

En novembre 2023, l'Autorité municipale des eaux d'Aliquippa, en Pennsylvanie, a été victime d'une cyberattaque ayant des implications internationales. Le samedi 25 novembre, un équipement informatique de l'autorité de l'eau, qui surveille la pression, a cessé de fonctionner, affichant à la place un message anti-israélien. La cyberattaque a été revendiquée par les Cyber Av3ngers, un groupe de cyber-criminel Iranien déjà impliqué dans des incidents similaires en Israël.



Le 23 décembre 2015, une cyberattaque de grande envergure a ciblé le réseau électrique ukrainien, laissant plus de 230 000 personnes sans électricité dans la région d'Ivano-Frankivsk. Le mode opératoire des cyber-criminels a d'abord ciblé le personnel de la centrale avec une campagne de spear-phishing contenant un document Word infecté par le malware BlackEnergy3. À l’activation de la macro par la victime, une porte dérobée est installée sur le poste de travail, permettant à l’attaquant d’accéder au réseau SCADA de la centrale électrique.

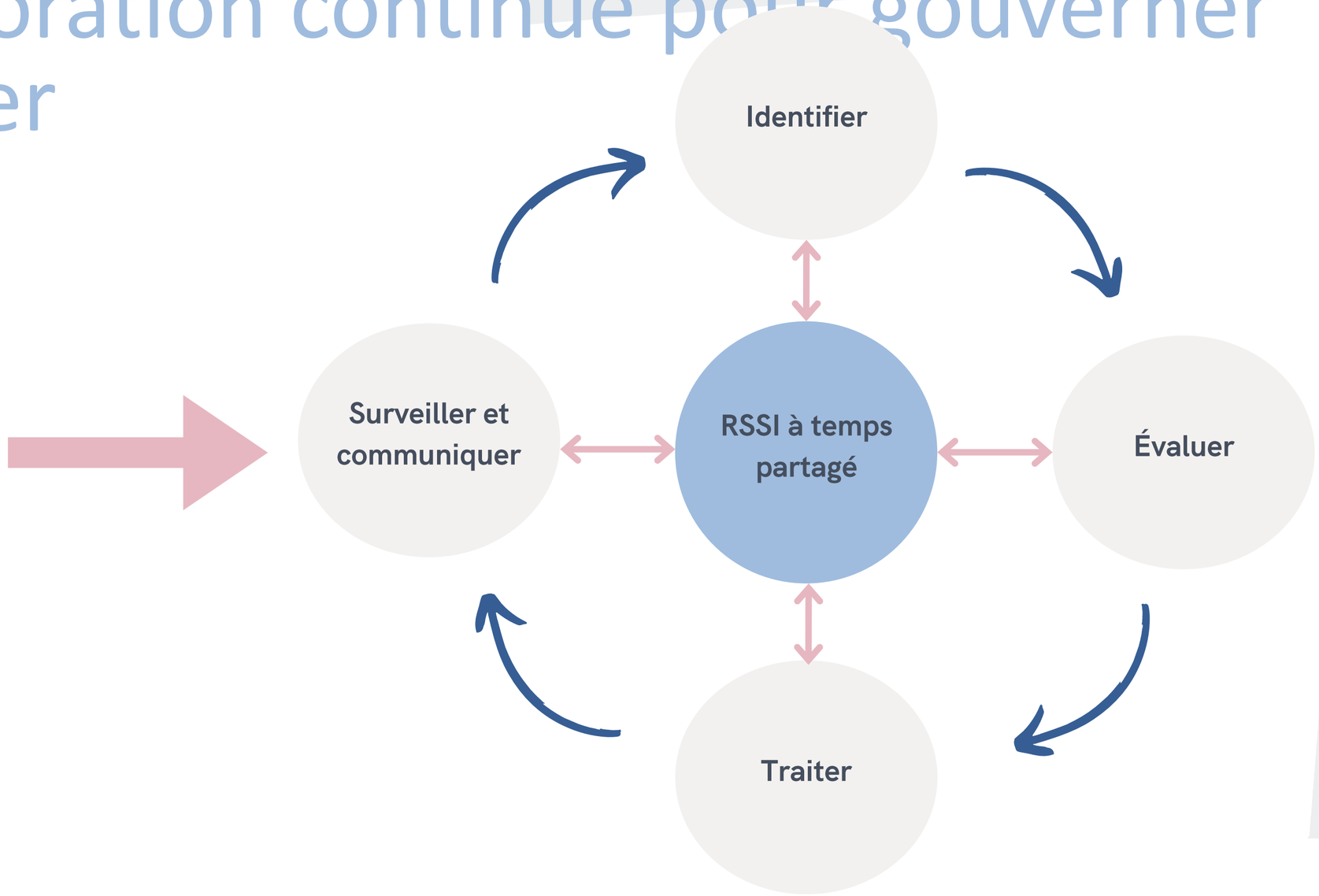


En France, en 2023, le Service public de l'assainissement francilien qui gère l’approvisionnement en eau des 9 millions d’habitants de la métropole du Grand Paris a déclaré avoir été victime d’une cyberattaque « étendue et virulente » visant le pilotage de ses réseaux et usines.

EVICYS
EXPERTS EN CYBERSÉCURITÉ

Le système de management du risque : un cycle d'amélioration continue pour gouverner le risque cyber

- Risques d'entreprise
- Audit
- Analyse de risque
- Vulnérabilités
- Incidents
- Tests d'intrusion



EVICYS
EXPERTS EN CYBERSÉCURITÉ

Notre offre

Pourquoi faire appel à un service RSSI à temps partagé ?

Les sociétés sont contraintes par des **exigences légales**

Il y a une forte difficulté à recruter à cause d'une **pénurie de talents**:

Recruter un RSSI coûte très cher : Selon le CESIN, le salaire moyen d'un RSSI est de 90 480€ brut, il dépasse les 120 000€ dans les grandes villes (Lyon, Paris, Marseille, Bordeaux)

EVICYS
EXPERTS EN CYBERSÉCURITÉ

Notre offre

Mise en place du service RSSI as a service

Le déploiement d'un service de Responsable de la Sécurité des Systèmes d'Information (RSSI) à temps partagé se déroule en deux phases principales : **la phase de construction (Build) et la phase d'exploitation (Run)**.

*La mise en place du service peut s'articuler avec l'intégration d'outils de **gouvernance** et de **monitoring.***

La phase de construction (Build)

Établir les fondations du système de gestion des risques et du RSSI. Cette phase consiste à réaliser un état des lieux approfondi de votre organisation en matière de sécurité et à définir les premières actions à mettre en œuvre.

La phase d'exploitation (Run)

Cette phase consiste à maintenir et à améliorer en continu le niveau de sécurité de votre organisation en s'appuyant sur les fondations posées lors de la phase de construction avec l'aide du RSSI As A Service.

EVICYS
EXPERTS EN CYBERSÉCURITÉ

EVICYS

EXPERTS EN CYBERSÉCURITÉ

Merci !

www.evicys.com contact@evicys.com 04 65 84 19 66

BCS Assurances

Risques de Fraude & Cyber

Les réponses apportées par les assurances Cyber-Fraude

Pour Tenerrdis & AURA Digital Solaire, le 5 décembre 2024

Pierre-Yves BORDEAUX, BCS Assurances

Py.bordeaux@gmail.com

06 51 06 5646

Pierre-Yves BORDEAUX – Fondateur/Dirigeant de BCS Assurances

Pierre-Yves possède 25 années d'expérience dans les métiers de la gestion des risques & des assurances, dans un environnement international :

- d'abord dans l'industrie (Lafarge-Holcim, Alcatel-Nokia)
- puis dans le courtage d'assurances (Aon France et Gras Savoye/Willis Towers Watson).

Je conseille des clients dans le secteur des Energies Renouvelables depuis plus de 20 ans et a été responsable France de ce secteur industriel pour le Groupe Gras Savoye/WTW pendant 5 ans, avant de créer BCS Assurances en janvier 2017.

BCS Assurances possède une double expertise :

1. Les assurances des SPV sous « Project Financed »
2. Les assurances de tous les acteurs de la chaîne de valeurs des ENR (not. RC).

BCS est un Adhérent de la 1ère heure de plusieurs Syndicats professionnels ENR, dont AURA Digital Solaire.

Pierre-Yves délivre des enseignements à Polytech Grenoble, l'Ecole des Mines de St-Etienne et Sc-Po Paris (Master NRJ).

Formation :

- Sciences-Po Grenoble
- Bordeaux Kedge (IMR)
- Associé en Risk Management (ARM)

Sommaire

1. En bref… sur les risques « cyber »
2. Exemples de sinistres dans les ENR
3. Les réponses des polices spécialisées
4. Conclusion

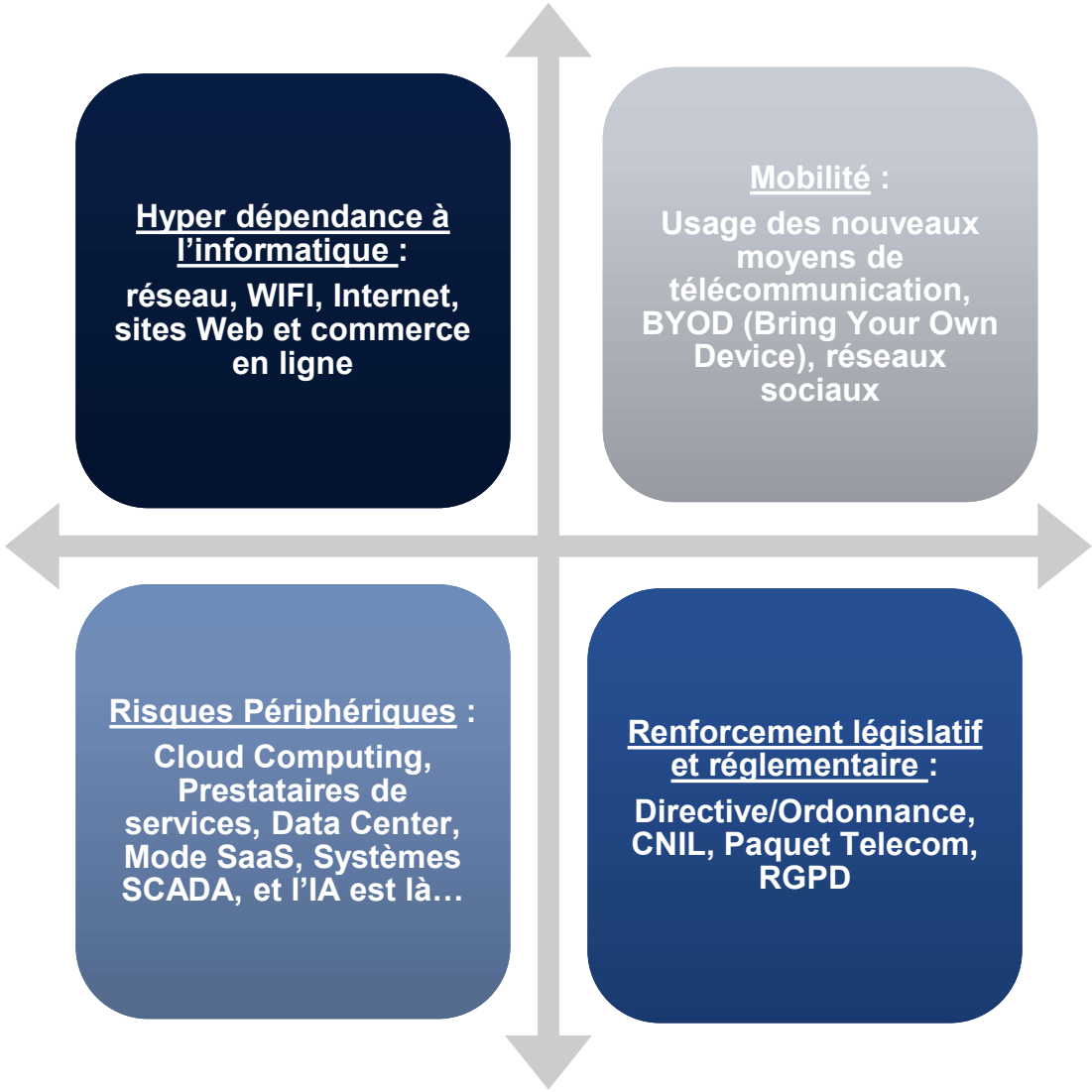
1. En bref… sur les risques cyber

Des vulnérabilités, une menace accrue et des responsabilités

Le fait que le progrès technique a toujours généré de nouveaux risques est encore plus vrai avec les cyber-technologies :

- Il est désormais facile et peu coûteux d'accéder à des outils de piratage.
- Dans le même temps, la marche inexorable de la numérisation des processus de production multiplie les aubaines offertes aux délinquants, sans parler de l'IA.
- Ajoutons le facteur humain, qui introduit inévitablement des failles partout où l'on n'a pas, en amont, pensé des dispositifs protecteurs mais coûteux.

Etre protégé par un anti-virus et par un fire-wall ne suffit plus. La question du cyber-crime n'est plus de savoir « si » mais « quand » il surviendra.



2. Exemples de sinistres dans les ENR

Quelques exemples de sinistres récents

Sinistre Sabella (10/2015)

- Entrée en service le mois précédent pour alimenter l'île d'Ouessant, l'hydrolienne Sabella D10 est bloquée par un virus "cryptolocker".
- Ce virus a piraté les serveurs de communication de la turbine (liaison Internet par satellite avec le centre de contrôle), neutralisant pendant quinze jours la connexion avec Quimper.
- L'attaque était accompagnée d'une demande de rançon de 4000 dollars. Que Sabella n'a pas payé.
- La société a examiné son système d'information pour débloquer toute seule le serveur de communication, renforcer la sécurité avec ses prestataires techniques et supprimer ce qu'elle pense avoir été la porte d'accès des pirates à son réseau.
- L'attaque démontre une fois de plus combien un lien réseau peut constituer une faille dans un système informatique.

Etude Tulsa (2017)

- Des chercheurs de l'université de Tulsa ont mené une expérience en piratant des parcs éoliens anonymes aux États-Unis en 2017 pour tester leurs vulnérabilités, avec l'autorisation des exploitants des parcs éoliens (rapport DNV).
- Les chercheurs ont crocheté une serrure pour accéder à une chambre située à la base d'une éolienne, indique le rapport. Ils ont accédé au serveur de l'éolienne et ont obtenu une liste d'adresses IP représentant chaque éolienne en réseau dans le champ. Ils ont ensuite empêché l'éolienne de tourner.

2. Exemples de sinistres dans les ENR

Quelques exemples de sinistres récents

Sinistre Eolien Terrestre (2022)

- En 2022, une cyberattaque a causé la mise en défaut du système de contrôle à distance de près de 11 GW d'éoliennes terrestres sur le sol allemand.
- Cette cyberattaque qui avait touché un réseau satellitaire, avait également engendré des coupures de connexion internet pour plusieurs milliers d'européens.

Sinistre en PV (S1/2024)

- Un pirate informatique néerlandais est parvenu à prendre le contrôle de 4 millions de centrales solaires photovoltaïques réparties dans 150 pays.
- Répondant au nom de Wietse Boonstra, ce « hacker éthique » a repéré une faille dans les logiciels internes d'Enphase (attaque de type DDOS). Au total, ce sont 6 vulnérabilités qui ont été découvertes. Si, lorsque le pirate a prévenu Enphase par l'intermédiaire de l'Institut néerlandais pour la divulgation de la vulnérabilité (DIVD), Enphase a réussi à corriger le problème en moins de 24 heures.

3. Les solutions des polices Cyber

3 blocs de garanties

2. Les risques d'atteintes aux SI/data appartenant à des tiers

(risques de RC dans le cadre d'une réclamation de tiers)

- Atteinte aux données personnelles et/ou confidentielles des Tiers (propriété intellectuelle)
- Interruption des services en ligne et réclamations de tiers (déni de service)
- Atteinte à la sécurité du réseau
- Garantie media / publication numérique dommageable
- Frais de Défense Externalisation / Sous-traitance

3. Services d'assistance et frais associés

(risques RC et Dommages aux biens)

- Hotline 24/24 Frais de notification/communication
- Frais d'experts en SI (Forensics) / Enquête, restauration des SI/Data + monitoring/surveillance
- Conseils juridiques / Frais de Défense
- Frais en cas d'enquête d'une autorité de contrôle / Sanctions pécuniaires (pénalités PCI DSS)
- Atteinte à l'image / gestion de crise (interne Groupe et ext. Médias)

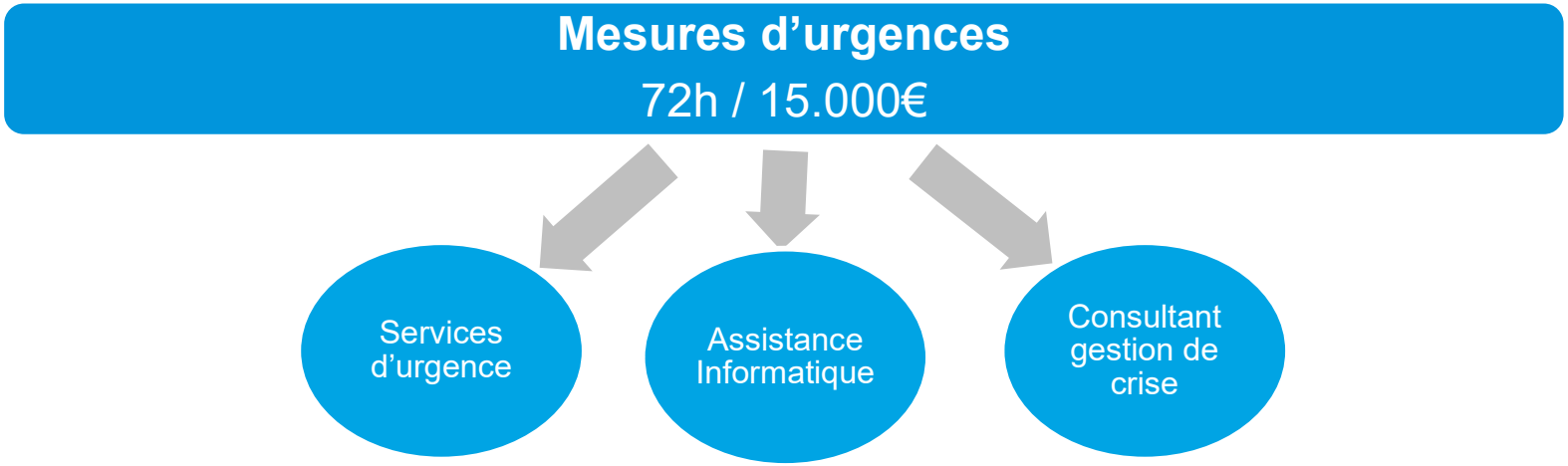
1. Les risques de Dommages aux biens appartenant à l'Assuré

(hardware, SI et data)

- Vol/Ajout, soustraction/extorsion, détérioration/destruction (défaçage, ransomware, erreur, incident IT…)
- + Impossibilité d'utilisation (cryptage) ou arrêt des SI/services cloud (déni de service site web)
- + Contamination des SI et des data (attaque logique, virus…)
- = Pertes d'Exploitation Consécutives (marge brute / charges fixes)
- = Frais supplémentaires d'exploitation (frais transfert vers un autre Presta.)

3. Les solutions des polices Cyber

Exemple de services d'assistance et d'avance de frais



Au delà

- Frais de notification
- Frais de monitoring & surveillance
- Frais d'atténuation du risque
- Frais de restauration des données

La réactivité est primordiale afin de limiter les conséquences préjudiciables d'une cyber-attaque !

3. Les solutions des polices Cyber

Les avantages de ce contrat

- Un process de cotation simple et rapide des garanties d'assurance
- De la réactivité dans la gestion des sinistres (ex. : notification dans les délais impartis en cas de piratage des données personnelles)
- Des primes peu élevées (marché spécifique mais dynamique)
- Se cumule avec des garanties fraude (fraude au président, détournement interne…).
- Intervient en complément des garanties existantes dans les polices « classiques » (Dommages et/ou Responsabilité Civile) qui sont :
  - généralement sous-limitées,
  - partiellement couvertes,
  - restreintes par des exclusions (cf. ci-après)

3. Les solutions des polices Cyber

Les « bonnes pratiques »

Les Cyber-risques ne sont pas isolés de l'exposition globale des risques :

- ils s'ajoutent aux risques existants, voir même les augmentent (atteinte à l'image)
- Ils doivent donc être traités par une approche préalable d'analyse et de traitement des risques.

Toute organisation souhaitant connaitre son exposition aux risques cyber devrait pratiquer un audit pour :

- En évaluer la fréquence et la gravité,
- Définir des scénarii hiérarchisés pour faciliter les arbitrages selon leur criticité,
- Aboutir à un plan de prévention/protection visant à réduire les risques à un niveau acceptable.

Exemples de « bonnes questions » :

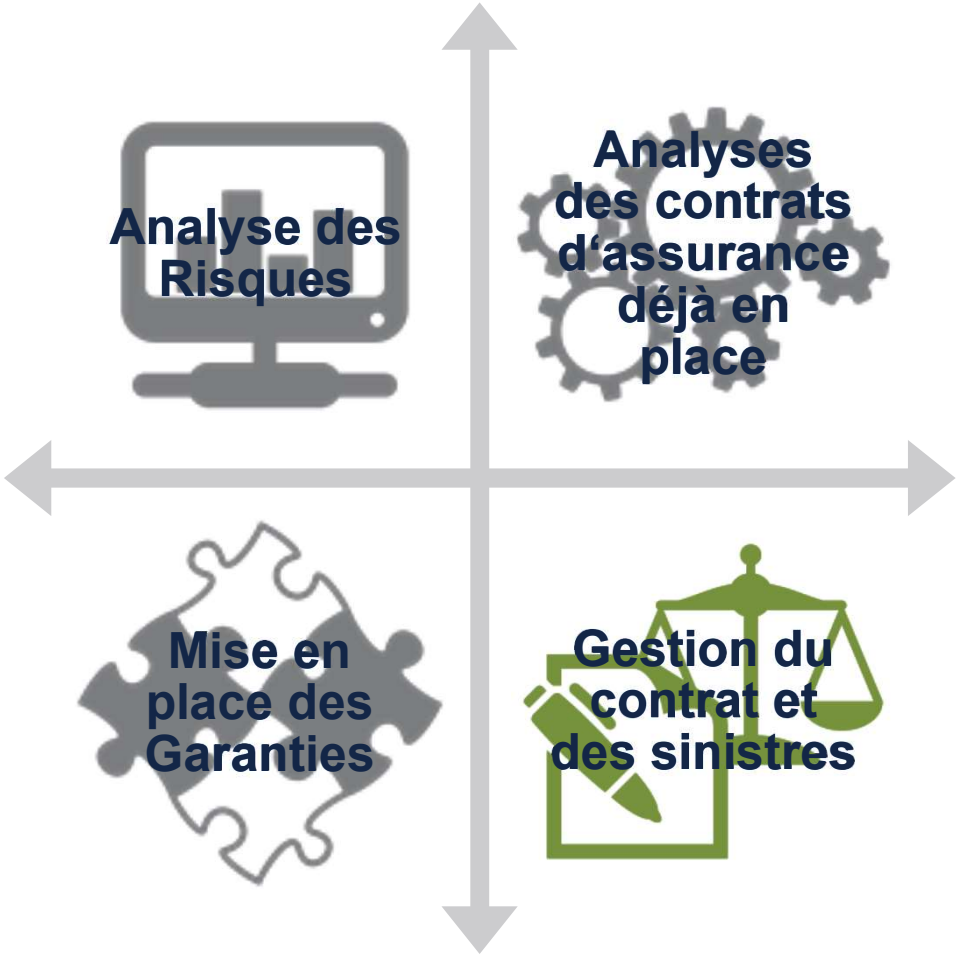
- Quel type d'interruption d'activité pourrait être déclenché par des disfonctionnements du matériel informatique ?
- Quelle « valeur » attribuez-vous aux données vous appartenant / appartenant aux Tiers ?
- Quel est le niveau d'engagement et de responsabilité vis-à-vis des tiers/parties prenantes : partenaires et fournisseurs ? (contrats en cours, externalisation…)
- Quels scenarii connexes de fraude : attaque par « social engineering » (fraude au président ou fournisseur connu) ?

4. Conclusion

Les solutions des polices Cyber

Le process de « Cyber risk management » devrait se dérouler selon les 4 étapes ci-jointes :

- Réaliser un diagnostic complet d'analyse des risques sur la protection des SI
- Définir une stratégie en matière de prévention-protection et de transfert des risques à l'assurance



BCS Assurances

Courtier spécialiste des Energies Renouvelables




Société de courtage d'assurance et de réassurance
Société par actions simplifiée au capital de 10.000,00 euros, immatriculée au RCS de Lyon sous le n°824 719 785

Siège social : 7 chemin caporal Ray 69140 Rillieux-la-Pape

Intermédiaire immatriculé à l'ORIAS sous le n°17000845 (http://www.orias.fr)
BCS Assurances est soumis au contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution)

sis 4, place de Budapest 75009 Paris.