World Energy Perspectives | 2016

SYNTHÈSE

WORLD ENERGY COUNCIL | CONSEIL FRANÇAIS DE L'ÉNERGIE

LE CHEMIN VERS LA RÉSILIENCE - GESTION DES CYBER-RISQUES

Une plus grande résilience aux cyber-risques est essentielle à la sécurité énergétique d'aujourd'hui et de demain. Internet et les technologies en réseau ont modifié de nombreux aspects du secteur de l'énergie. Le développement de la digitalisation par des équipements comme les compteurs intelligents est source d'efficacité et donne aux exploitants l'opportunité d'améliorer la gestion du réseau, la gestion des pipelines, ainsi que l'exploration et la production. Mais, avec ces avantages, apparaissent des vulnérabilités croissantes, en particulier à cause de l'automatisation des systèmes de contrôle industriels (SCI). Des attaques menées sur les SCI pourraient entraîner la perte de contrôle d'équipements-clés, ce qui pourrait causer des dommages dans le monde réel. Cela pourrait notamment entraîner des pannes de machines, des incendies, des explosions ou des blessures, avec d'importantes répercussions sur l'activité des infrastructures énergétiques, des populations locales et de l'économie.

Ce rapport étudie la manière de mieux gérer les cyber-risques en tenant compte des évolutions du secteur de l'énergie et des infrastructures énergétiques. En s'appuyant sur les connaissances d'un réseau de spécialistes du secteur de l'énergie, il examine l'évolution des vulnérabilités des infrastructures énergétiques, existantes ou nouvelles et recommande des mesures que les décideurs et les parties prenantes dans le domaine de l'énergie peuvent prendre, à titre individuel et en collaboration, pour améliorer la réponse du secteur à l'apparition de cyber-menaces, dans le cadre d'une démarche plus large vers une plus grande résilience.

PRINCIPALES CONCLUSIONS

1 **LES CYBER-MENACES FONT PARTIE DES PRINCIPALES PRÉOCCUPATIONS** des dirigeants du secteur de l'énergie, surtout dans les pays à forte maturité des infrastructures et, plus particulièrement, en Amérique du nord et en Europe. Dans ces régions, les dirigeants de l'énergie reconnaissent de plus en plus qu'il est important de considérer les cyber-attaques comme une menace fondamentale pour la continuité de l'activité et qu'il est nécessaire d'instaurer, dans toute l'organisation, une sensibilité culturelle aux nouvelles technologies qui dépasse les départements de traitement de l'information.

2 **LES INTERCONNEXIONS ET LA DIGITALISATION CROISSANTES** du secteur énergétique — réseaux intelligents, équipements intelligents et développement de l'Internet des objets, y compris les objets connectés — et son rôle essentiel dans le fonctionnement d'une économie moderne font de ce secteur une cible de premier choix pour les cyber-attaques visant à perturber l'exploitation. Bien que la digitalisation améliore l'efficacité de l'exploitation, le développement des interconnexions accroît également la complexité de la gestion des cyber-risques.

3 **LES CYBER-RISQUES SONT UNE PRÉOCCUPATION EXCEPTIONNELLE** dans le secteur énergétique, parce qu'une attaque menée contre une infrastructure énergétique peut devenir réelle et provoquer, par exemple, une défaillance à grande échelle dans l'exploitation d'une infrastructure énergétique. Les grandes infrastructures centralisées sont particulièrement menacées en raison d'un potentiel « effet domino » qu'une attaque pourrait entraîner sur une centrale nucléaire, à charbon ou à fioul.

4 **LES FOURNISSEURS DE TECHNOLOGIE PEUVENT JOUER UN RÔLE ESSENTIEL** pour développer ou limiter la résilience des infrastructures énergétiques. Ces entreprises doivent garantir la fourniture de technologies intégrant des normes de sécurité à leurs produits. Dans le cas contraire, les SCI et les systèmes de contrôle et d'acquisition de données peuvent aggraver les cyber-risques et accroître la vulnérabilité des exploitations énergétiques aux attaques.

5 **LES ENTREPRISES RECONNAISSENT DE PLUS EN PLUS LA DIGITALISATION** comme un risque fondamental. Les échanges d'informations entre les membres d'un même secteur et entre les différents secteurs à propos de leurs expériences en matière de cyber-risques sont insuffisants. Améliorer les échanges d'informations au sein du secteur et entre parties prenantes publiques et privées permettrait de mieux comprendre l'impact des cyber-risques sur les entreprises de l'énergie et sur le secteur énergétique dans son ensemble. De plus, la sensibilisation des employés aux cyber-vulnérabilités doit s'inscrire dans une stratégie de cyber-sécurité efficace. L'erreur humaine est très souvent un facteur déterminant de la réussite des cyber-attaques parce que le personnel, à tous les niveaux de l'entreprise, n'a pas une connaissance suffisante des cyber-risques.

6 **LA CYBER-ASSURANCE EST UN DISPOSITIF** qui permet d'aider à compenser les éventuelles pertes financières occasionnées par une cyber-attaque. Cependant, le secteur des assurances doit continuer à développer des instruments pour pouvoir faire face à des pertes potentiellement catastrophiques et à la complexité des cyber-risques. Comme tout risque émergent et évolutif, on dispose d'assez peu de données historiques sur les cyber-risques; cela limite la maturité du marché des cyber-assurances. Néanmoins, faire la démarche de souscrire une cyber-assurance est en soi souvent bénéfique pour les entreprises, car cela les oblige à évaluer leurs cyber-pratiques.

IMPLICATIONS POUR L'ÉNERGIE

Comme le secteur de l'énergie cherche à améliorer son efficacité et sa fiabilité, les exploitants d'infrastructures doivent être conscients que l'utilisation accrue de l'Internet des objets augmente également la vulnérabilité aux cyber-attaques sur toute la chaîne de valeur de l'énergie.

Les cyber-risques ne doivent pas être considérés purement comme des risques informatiques mais doivent être traités comme un problème qui concerne l'entreprise toute entière et comme un risque d'exploitation exigeant une gestion des risques efficace et globale et notamment la gouvernance et la supervision du Conseil d'administration et de l'équipe de Direction.

Le secteur de l'énergie doit adopter une approche systémique et évaluer les cyber-risques sur l'ensemble de la chaîne d'approvisionnement énergétique afin d'améliorer la protection des systèmes énergétiques et de limiter les possibles effets domino pouvant être provoqués par la défaillance d'un élément de la chaîne de valeur. Néanmoins, les mesures qui requièrent la conformité de la chaîne d'approvisionnement ou une coopération transfrontalière sont plus difficiles à mettre en place et nécessitent une collaboration accrue entre les secteurs.

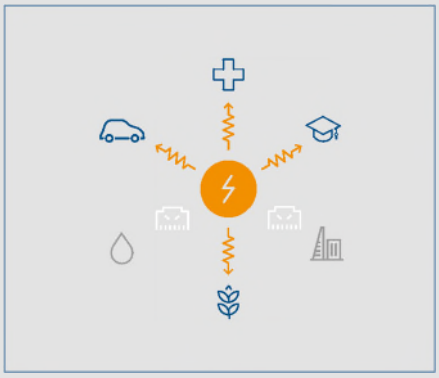
Les entreprises doivent appliquer des mesures de prévention, de détection et de réaction aux cyber-attaques. Cela inclut à la fois des mesures de résilience techniques (des mesures de sécurité pour les logiciels et le matériel, des mesures régissant les structures physiques comme la limitation de l'accès aux centres de données et des instructions claires concernant l'utilisation des disques durs externes), et des mesures de résilience humaine construite sur le développement d'une solide sensibilité culturelle aux nouvelles technologies dans les organisations et au-delà.

Travailler avec d'autres secteurs et collaborer avec des institutions gouvernementales et privées peut aider les entreprises à mieux comprendre la nature des impacts des cyber-risques. La coopération internationale doit être développée pour renforcer la cyber-sécurité et la résilience des systèmes énergétiques. Il est essentiel de diffuser des informations sur les incidents, de partager les meilleures pratiques et de définir des normes internationales de cyber-sécurité pour relever ce défi.

Si le secteur de l'énergie et des utilités met en place des mesures de protection des risques et de résilience, les professionnels de la finance et des assurances seront en mesure de proposer des couvertures en cas de sinistres à des prix raisonnables. Les cyber-attaques dans le secteur de l'énergie ont des conséquences non seulement sur le secteur lui-même, mais sur l'ensemble de l'économie et sur tout le tissu industriel d'une nation. En outre, comme la technologie informatique et les vecteurs des cyber-menaces changent constamment, en partie pour développer des moyens de défense, les assureurs vont être confrontés à la difficulté de devoir évaluer avec précision l'impact des cyber-attaques ; les données historiques pourraient ne pas être suffisantes. Une meilleure communication des informations de la part du secteur de l'énergie aidera les compagnies d'assurance à améliorer leur couverture des actifs énergétiques. Toutefois, les entreprises du secteur de l'énergie doivent aussi identifier plus clairement là où une assurance est le plus utile pour satisfaire leur besoin de protection et elles doivent travailler en collaboration avec les assureurs pour continuer à développer des produits de cyber-assurance.

LE CHEMIN VERS LA RÉSILIENCE - LA GESTION DES CYBER-RISQUES

LES INFRASTRUCTURES ÉNERGÉTIQUES : LE COEUR DE TOUTES LES ÉCONOMIES MODERNES

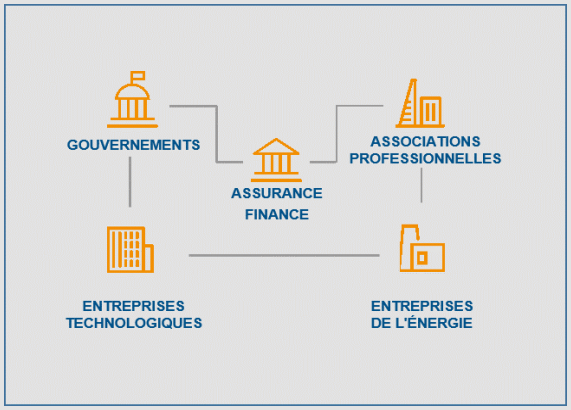


Les cyber-risques sont de plus en plus complexes et les attaques de plus en plus fréquentes. Les conséquences physiques et économiques des cyber-attaques sur les infrastructures énergétiques peuvent être graves, ce qui en fait des cibles attractives.

RECOMMANDATIONS

Toutes les parties prenantes doivent collaborer dans les quatre domaines suivants pour aborder les cyber-risques :

- Les facteurs techniques et humains
- Le partage des informations sur les cyber-risques
- L'évaluation et la quantification des risques
- L'établissement de normes et le partage des meilleures pratiques



ÉTUDES DE CAS

❶ ÉTATS-UNIS ET CANADA, 2013–2015

PRODUCTION D'ÉLECTRICITÉ
Erreur humaine // Piratage informatique

Cette attaque menée sur Calpine qui exploite 82 centrales électriques aux États-Unis et au Canada a commencé par le vol d'informations chez un sous-traitant. Des *hackers* sont parvenus à voler des informations essentielles sur les plans des centrales et sur les systèmes de mots de passe.

❷ ÉTATS-UNIS, 2003

CENTRALE NUCLÉAIRE
Logiciel malveillant

Slammer a été le ver informatique le plus rapide de l'histoire. En 2003, il a attaqué le réseau privé d'une centrale nucléaire inactive dans l'Ohio et a désactivé un système de surveillance et de sécurité pendant 5 heures. Cinq autres utilités ont également été affectées.

❸ ÉTATS-UNIS, 2012

PRODUCTION D'ÉLECTRICITÉ
Erreur humaine // virus

Aux Etats-Unis, le SCI d'une utilité a été infecté par le virus Mariposa quand un technicien extérieur s'est servi d'une clé USB infectée pour télécharger un logiciel sur les systèmes. Ce virus a entraîné une panne des systèmes et a retardé le redémarrage de la centrale d'environ 3 semaines.

❹ ÉTATS-UNIS, 2013

INFRASTRUCTURES NON ÉNERGÉTIQUES
Logiciel malveillant

Le petit barrage de Bowman Avenue, près de New York, sert davantage à contrôler les inondations qu'à produire de l'électricité. Des *hackers* sont parvenus à accéder partiellement aux systèmes de ce barrage à l'aide d'un logiciel malveillant standard, mettant ainsi en évidence la vulnérabilité de l'ensemble des infrastructures.

❺ UKRAINE, 2015

RÉSEAU ÉLECTRIQUE
Piratage informatique // erreur humaine

Ce piratage bien planifié de trois sociétés de distribution d'électricité a entraîné des coupures chez 80 000 consommateurs. C'est le premier piratage connu ayant provoqué une coupure de courant. Le piratage a commencé par une campagne de hameçonnage qui ciblait le personnel du service informatique des entreprises.

⑥ ARABIE SAOUDITE, 2012

COMPAGNIE PÉTROLIÈRE

Virus

Le virus *Shamoon* a infecté 30 000 ordinateurs appartenant à Saudi Aramco, le plus grand producteur mondial de pétrole et de gaz. Certains systèmes n'ont plus eu de connexion pendant 10 jours et 85% du matériel informatique de la société a été détruit. L'économie nationale toute entière a été touchée.

⑦ PAYS-BAS, 2012

TÉLÉCOMMUNICATIONS

Piratage informatique

Un adolescent de dix-sept ans a été arrêté pour avoir pénétré dans des centaines de serveurs. La maintenance de ces serveurs était effectuée par une société de télécommunications assurant des prestations de « smart metering » pour des utilités.

⑧ ALLEMAGNE, 2014

EQUIPEMENT

Piratage informatique

Les pirates informatiques ont attaqué le réseau commercial d'une aciérie allemande et, à partir de là, son réseau de production, provoquant d'énormes dégâts au niveau de ses équipements industriels. C'était la deuxième cyber-attaque connue qui touchait une infrastructure physique.

⑨ ISRAËL, 2016

SECTEUR PUBLIC; RÉSEAU ÉLECTRIQUE Logiciel malveillant // erreur humaine

Un employé de la Régie d'électricité a subi une attaque par hameçonnage, qui a infecté un certain nombre d'ordinateurs sur le réseau avec un logiciel malveillant. Le réseau électrique n'a pas été affecté, mais il a fallu deux jours à la Régie d'électricité pour rétablir un fonctionnement normal.

⑩ CORÉE DU SUD, 2015

CENTRALE NUCLÉAIRE

Piratage informatique

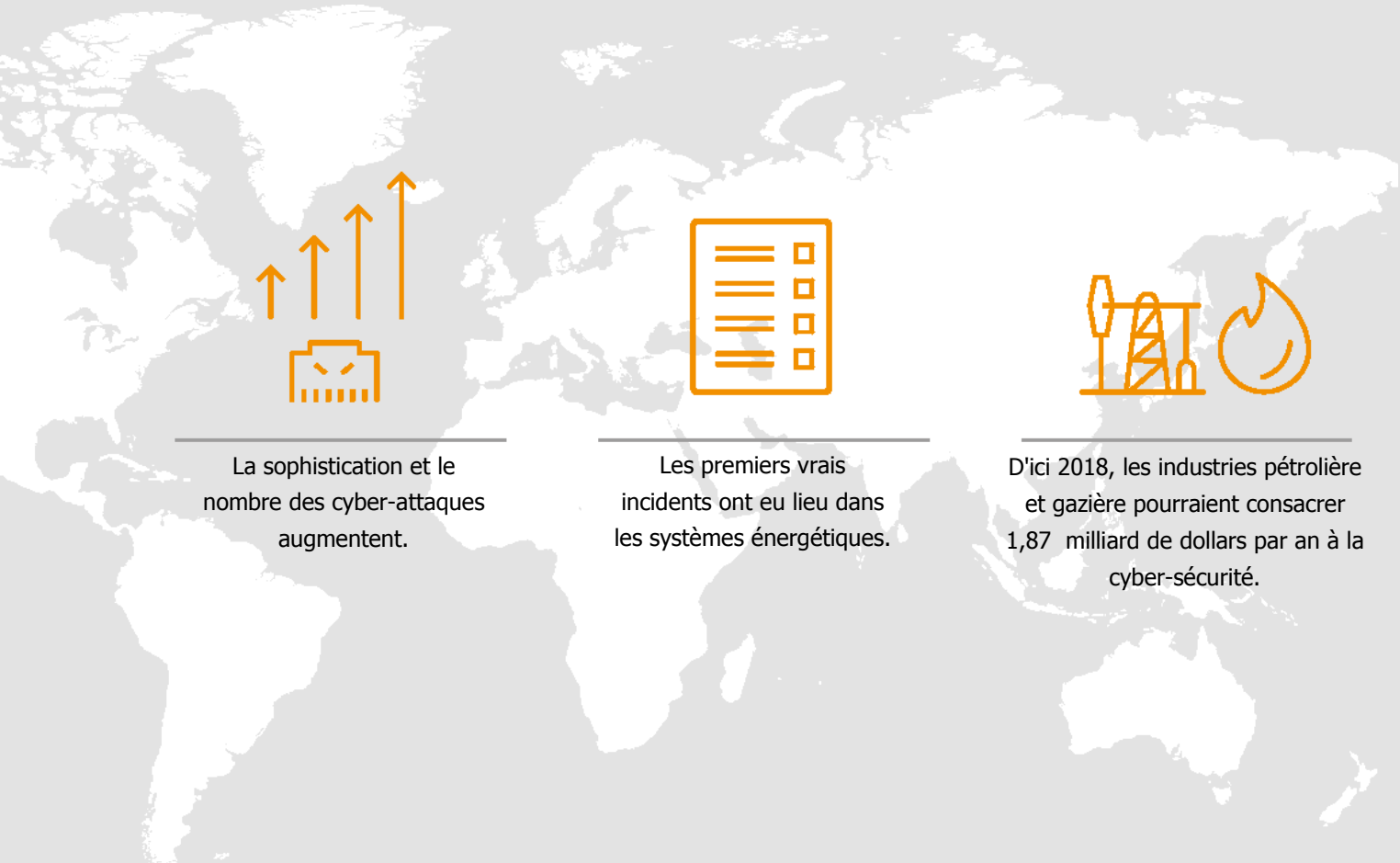
Korea Hydro et Nuclear Power ont subi une série d'attaques visant à provoquer des dysfonctionnements des réacteurs nucléaires. Les attaques ont seulement réussi à divulguer des documents non classifiés.

⑪ AUSTRALIE, 2015

SECTEUR PUBLIC

Piratage informatique // virus

Les pirates informatiques ont attaqué le bureau de Maitland du Ministère des Ressources et de l'Énergie en Nouvelle-Galles du Sud. Les hackers étaient peut-être intéressés par les projets en cours de ce Ministère, ou peut-être le considéraient-ils comme un maillon faible qui pouvait leur permettre d'accéder à des informations gouvernementales d'un niveau de classification beaucoup plus important.



La sophistication et le nombre des cyber-attaques augmentent.

Les premiers vrais incidents ont eu lieu dans les systèmes énergétiques.

D'ici 2018, les industries pétrolière et gazière pourraient consacrer 1,87 milliard de dollars par an à la cyber-sécurité.

RECOMMANDATIONS

Toutes les parties prenantes doivent jouer un rôle actif dans la gestion des cyber-risques :

► **Le secteur de l'assurance et de la finance** doit adapter la couverture pour répondre à l'évolution permanente des cyber-risques. Ce secteur doit collaborer avec le secteur de l'énergie pour améliorer la connaissance des produits de cyber-assurance, pour développer davantage le marché de la cyber-assurance et, parallèlement, pour soutenir le secteur de l'énergie en déterminant et en rassemblant des données essentielles relatives aux cyber-risques. Ce secteur doit rester informé de la constante évolution des développements technologiques qui détermineront les risques à garantir. Il doit suivre les cyber-risques couverts par les produits d'assurance existants et s'adapter le cas échéant, en termes de prix ou de restrictions par exemple, et se concentrer sur la gestion des risques nouveaux et des risques de cumul. Enfin, le secteur de l'assurance et de la finance doit répondre aux exigences en constante évolution de « cyber régulation ».

► **Les entreprises spécialisées dans l'énergie** doivent considérer les cyber-risques comme des risques d'entreprise majeurs, évaluer efficacement et comprendre les cyber-risques spécifiques à leur entreprise et élaborer de solides stratégies de résilience techniques et humaines. Les entreprises doivent s'attacher entre autres à sensibiliser d'autres parties prenantes du secteur de l'énergie à l'impact des cyber-attaques; cela garantira l'intégration de la communauté de l'énergie, au sens large, dans les mesures de résilience.

► **Les gouvernements** doivent aider les entreprises à réagir fortement aux cyber-risques en incitant à la mise en place de normes ou en imposant une réglementation spécifique. Cependant, les exigences en matière de réglementation et de suivi ne doivent pas devenir trop complexes par rapport à ce risque dynamique. Les gouvernements doivent encourager le partage des informations entre les pays, les secteurs et au sein de l'industrie, et ils doivent améliorer la coopération internationale sur la cyber-sécurité.

► **Les sociétés spécialisées dans les technologies pour le secteur énergétique** doivent intégrer les caractéristiques et les préoccupations de sécurité lorsqu'elles développent des technologies et collaborer avec le secteur de l'énergie afin d'utiliser les technologies les plus récentes pour contrôler la nature des cyber-attaques.

► **Les associations professionnelles** doivent soutenir et encourager le partage des informations et l'adoption des meilleures pratiques, conduire des évaluations par les pairs, et aider les entreprises et le secteur à développer une culture solide et active de la connaissance des nouvelles technologies.

Version originale anglaise publiée par le Conseil Mondial de l'Énergie, enregistré en Angleterre et au Pays de galles No. 4184478, Registered Office, 62–64 Cornhill, London EC3V 3NH, United Kingdom

Directeur de la publication : Jean Eudes Moncomble, Secrétaire général du Conseil Français de l'Énergie, Conseil Français de l'Énergie, 12 rue de Saint-Quentin – 75010 Paris – www.wec-france.org