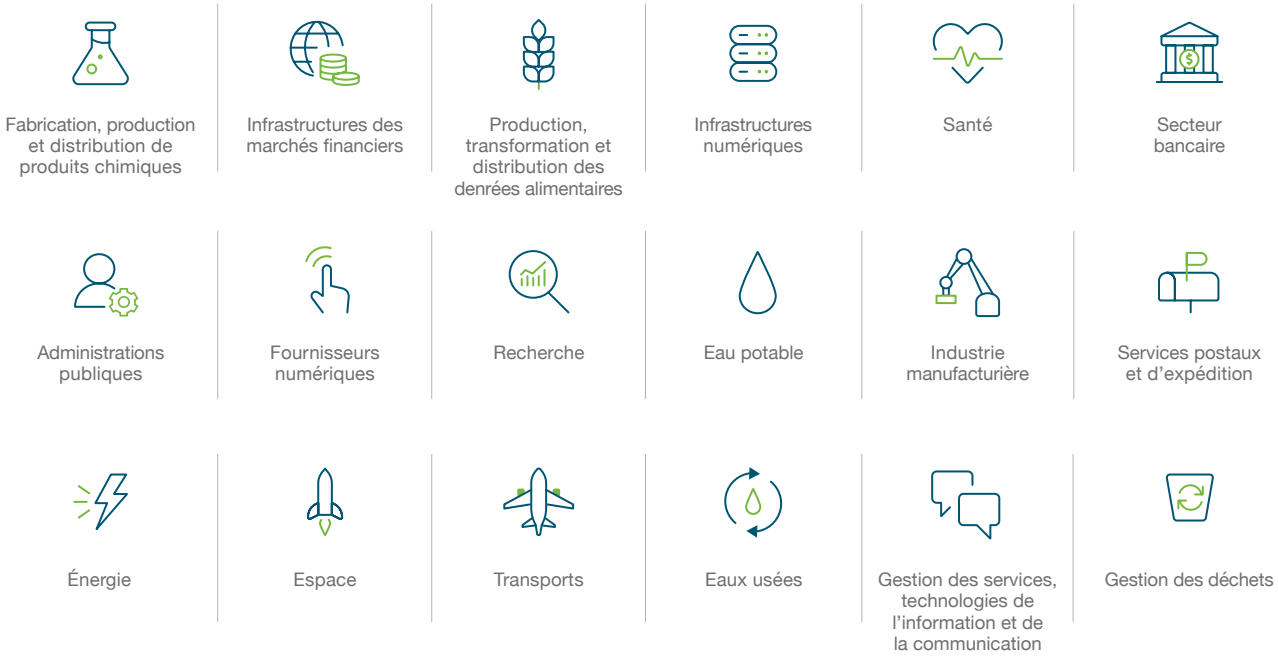
Dirigeants d’entreprise : la sécurisation des infrastructures stratégiques commence par vous et repose sur le MFA résistant au phishing

De plus en plus de cybercriminels tentent de perturber la vie et la sécurité publiques en ciblant les infrastructures stratégiques. Une bonne culture de la cybersécurité commence par vous, leader d‘une entreprise stratégique.

Votre entreprise est-elle considérée comme stratégique ?

Les infrastructures stratégiques peuvent être définies comme les réseaux et les systèmes d’information servant à fournir des services essentiels dans les secteurs clés de nos sociétés. La directive NIS2 distingue deux catégories d’entités régulées : les entités essentielles (EE) et les entités importantes (EI). Cette catégorisation s’établit selon leur degré de criticité, leur taille et leur chiffre d’affaires (pour les entreprises).

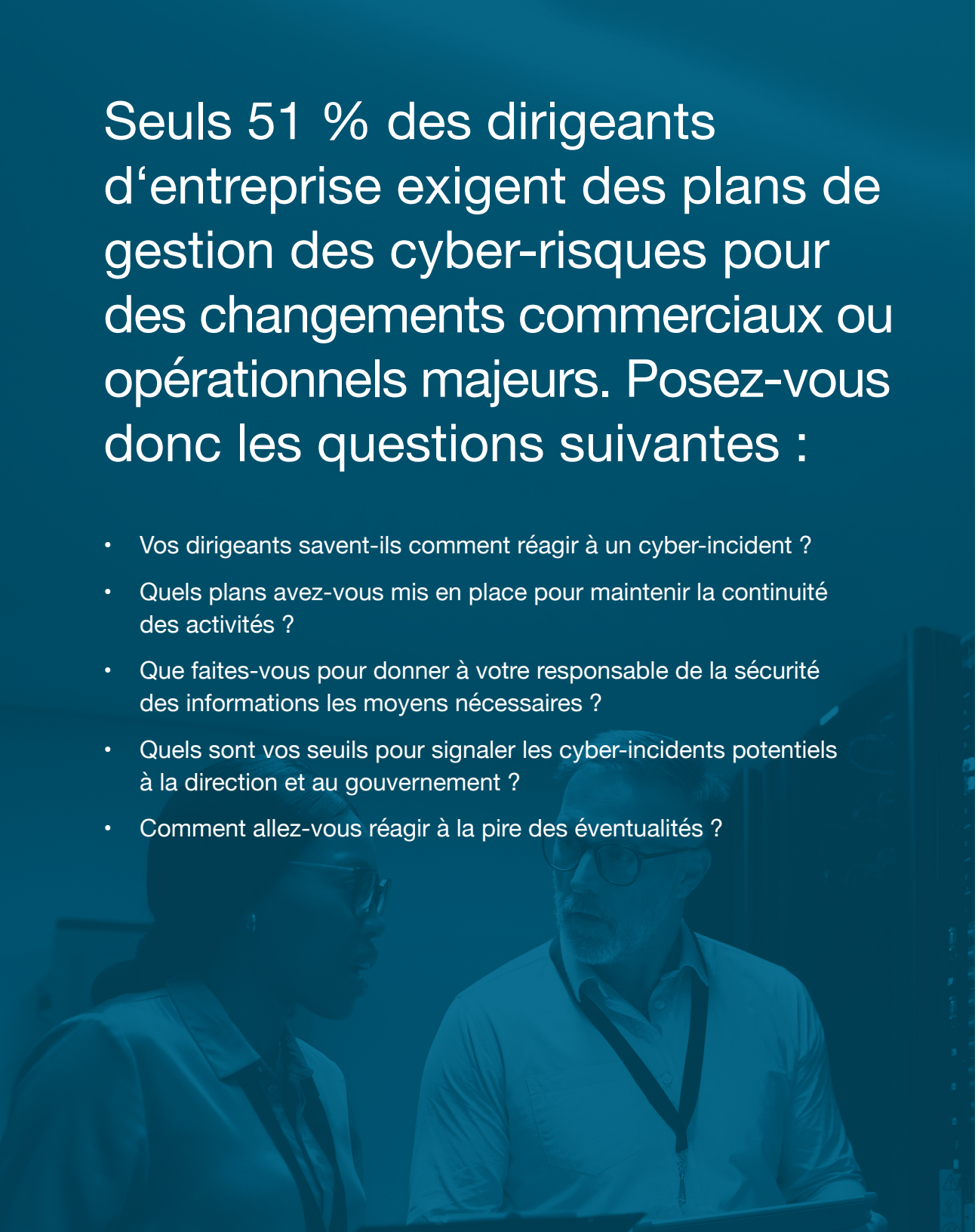
Mon Espace NIS2



yubico

Seuls 51 % des dirigeants d'entreprise exigent des plans de gestion des cyber-risques pour des changements commerciaux ou opérationnels majeurs. Posez-vous donc les questions suivantes :

- Vos dirigeants savent-ils comment réagir à un cyber-incident ?
- Quels plans avez-vous mis en place pour maintenir la continuité des activités ?
- Que faites-vous pour donner à votre responsable de la sécurité des informations les moyens nécessaires ?
- Quels sont vos seuils pour signaler les cyber-incidents potentiels à la direction et au gouvernement ?
- Comment allez-vous réagir à la pire des éventualités ?



La preuve indéniable que les cyber-menaces ciblant les infrastructures stratégiques sont bel et bien réelles :

40 %

Les cyberattaques ciblant des infrastructures stratégiques dans le monde entier **sont passées de 20 % de** toutes les attaques visant des États-nations **à 40 %** (Source)

25 %

40 % des 500 fournisseurs d'infrastructures stratégiques américains interrogés ont déclaré que les cybercriminels avaient tenté de fermer leurs systèmes de contrôle (Source)

80 %

Près de 80 % des entreprises à infrastructure stratégique étudiées dans un rapport d'IBM de 2022 n'ont pas adopté de stratégies Zero Trust. Conséquence : une augmentation moyenne des coûts liés aux brèches de données à 5,4 millions de dollars, soit 1,17 million de dollars de plus que celles en ayant mis en place (Source)

$9.23 million

C'est dans le secteur de la santé que le coût total moyen est le plus élevé en cas de brèche de données : **9,23 millions de dollars** (Source)

89 %

89 % des entreprises du secteur de l'électricité, du pétrole et du gaz et de la fabrication ont subi des cyberattaques qui ont eu un impact sur la production et l'approvisionnement en énergie entre le milieu de l'année 2021 et le milieu de l'année 2022 (Source)

yubico

La stratégie de continuité d'activité de chaque PDG doit commencer par un MFA résistant au phishing

Une partie essentielle de la réussite d'une stratégie de cybersécurité repose sur l'authentification multi-facteurs (MFA) et les passkeys matérielles, mais toutes les formes de MFA ne sont pas identiques. L'authentification moderne résistante au phishing et la sécurité matérielle constituent les meilleurs moyens de protéger les informations, les processus et les systèmes informatiques et OT stratégiques dont dépend notre société. C'est la raison pour laquelle elle est devenue la norme pour les organismes gouvernementaux et un nombre croissant d'organismes de réglementation.

Pour découvrir comment les secteurs stratégiques mettent en œuvre cette stratégie au sein de leurs entreprises, de leur chaîne logistique et dans le monde entier, lisez ceci :

Un État américain utilise les YubiKey pour protéger les bases de données d'enregistrement des électeurs contre les pirates

LIRE L'ÉTUDE DE CAS

yubi.co/USGovernment

Schneider Electric renforce la sécurité de sa chaîne d'approvisionnement mondiale avec des YubiKey et YubiHSM

LIRE L'ÉTUDE DE CAS

yubi.co/SchneiderElectric

Les YubiKeys défendent la compagnie pétrolière et gazière nationale ukrainienne contre les cyberattaques

LIRE L'ÉTUDE DE CAS

yubi.co/Naftogaz

yubico

Dans un monde interconnecté, nous sommes toutes et tous responsables du renforcement de l'écosystème de cybersécurité

« Le facteur humain représente l'une des plus grandes menaces de cybersécurité, par le biais d'attaques par phishing, lorsque les cybercriminels obtiennent des mots de passe ou des identifiants. »

Oleksandr Tarasov

Responsable des contrôles de sécurité au centre des opérations de sécurité, Naftogaz-Bezreka (compagnie pétrolière et gazière nationale ukrainienne)

Yubi.co/Naftogaz

10 % de toutes les brèches concernent les services financiers (Source)

11 États aux États-Unis ont subi des pannes de gaz temporaires lors de l'attaque par ransomware ayant visé Colonial Pipeline en 2021 (Source)

Les incidents de cybersécurité ayant un impact sur les infrastructures stratégiques australiennes ont augmenté de près d'un tiers au cours de l'exercice 2022-2023 (Source)

Les cybercriminels ont mis hors ligne la bourse polonaise (Source)

Les infrastructures, industries et agences gouvernementales stratégiques japonaises ont toutes constaté une augmentation des cyberattaques (Source)

Yubico (Nasdaq First North Growth Market Stockholm : YUBICO) est l'inventeur de la YubiKey, la référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, et un créateur et contributeur des standards d'authentification ouverts FIDO. C'est un pionnier de l'authentification sans mot de passe à l'aide des passkeys les plus fiables, avec des clients dans plus de 160 pays. Pour en savoir plus, rendez-vous sur www.yubico.com.

Contactez-nous
yubi.co/contact-fr

yubico