ISO focus
#132
L'actualité incontournable des Normes internationales

Les cyber-**secrets**

#132

ISO focus

Janvier-février 2019

ISOfocus Janvier-février 2019 – ISSN 2226-1109

ISOfocus, le magazine de l'Organisation internationale de normalisation, paraît six fois par an. Vous trouverez des compléments d'infos sur notre site Web à l'adresse **iso.org/isofocus** ou en nous suivant sur :

Chef, Communication | **Katie Bird**

Rédactrice en chef | **Elizabeth Gasiorowski-Denis**

Auteur | **Barnaby Lewis**

Contributeurs | **Robert Bartram, Rick Gould**

Éditrice et Lectrice d'épreuves | **Vivienne Rojas**

Graphistes | **Xela Damond, Pierre Granier, Alexane Rosa**

Traductrice | **Alexandra Florent**

Abonnements et anciens numéros

Si vous aimez *ISOfocus*, vous pouvez télécharger gratuitement le fichier pdf ou vous abonner sur notre site Web à **iso.org/isofocus** pour recevoir le magazine sur papier. Vous pouvez également contacter notre service à la clientèle à l'adresse **customerservice@iso.org**.

Contributions

Vous pouvez participer à la création de ce magazine : si vous pensez que votre contribution pourrait apporter un plus à l'une ou l'autre de nos rubriques, n'hésitez pas à nous contacter à **isofocus@iso.org**.
Les articles publiés représentent le point de vue de leurs auteurs et ne reflètent pas nécessairement celui de l'ISO ou de l'un de ses membres.

MIXTE Papier issu de sources responsables FSC® C008839

Ce magazine est imprimé sur du papier certifié FSC®.

myclimate neutral imprimé 01-14-277370 myclimate.org

Continuer à œuvrer avec CONFIANCE

***John Walter**, Président de l'ISO.*

Au terme de ma première année de présidence de l'ISO, j'éprouve une grande fierté et un véritable sens du devoir accompli. Pour revenir sur l'année écoulée – en fait, sur la dernière décennie – il est impressionnant de voir l'ampleur de tout ce que l'ISO a réalisé et les bons résultats obtenus. Ces résultats ne concernent pas seulement nos solides processus d'élaboration de normes et nos livrables, ils touchent aussi aux moyens qui nous ont permis d'apporter aide et conseils à bon nombre de nos membres dans le monde entier.

J'ai déjà dit à plusieurs reprises à quel point, dans le monde entier, les normalisateurs sont des exemples extraordinaires d'amitié, de coopération, de confiance et de relations de travail collégiales. Nous ouvrons des portes et construisons des ponts. Nous établissons et entretenons des partenariats de confiance. Nous respectons et valorisons chaque personne et chaque organisme national de normalisation. Nous n'exerçons de discrimination à l'encontre d'aucune personne, organisation ou nation. Nous accueillons et acceptons tous les participants qui manifestent un engagement sincère à la cause des Normes internationales et à leur utilisation au profit de notre village planétaire. Le monde a besoin de davantage d'ISO.

Pour cette raison, nous avons tous l'obligation de maintenir l'ISO et de la cultiver en tant qu'organisation dynamique en pleine santé. Le monde n'attend rien de moins de nous. Lorsque je rencontre des dirigeants de l'industrie et des gouvernements dans toutes les parties du monde, je suis chaleureusement accueilli. Tous cherchent ardemment des solutions face à des défis sérieux et graves. Nous passons souvent du temps à décrire et à examiner les options qu'offrent les Normes internationales, et à l'issue de ces séances, tous sont unanimes à vouloir travailler avec l'ISO, et y apporter leur collaboration, leur coopération et leur soutien. Un tel engagement de leur part m'encourage grandement et c'est l'une des raisons pour lesquelles le Secrétaire général, Sergio Mujica, et moi-même continuons de poursuivre nos échanges fructueux avec les principaux dirigeants de la planète.

Nous devons cependant faire plus – nous devons faire un travail de sensibilisation et de mobilisation. Nous devons continuer à fournir des solutions. L'avenir de ce monde dépend peut-être de nous. La construction de valeur pour nos membres est un élément clé pour Sergio comme pour moi. Je suis très heureux de la façon dont nous avons tenu nos engagements et de la façon dont nous avons su impliquer la communauté à l'échelle mondiale. À la tête de l'Organisation, Sergio s'exprime avec compétence, intelligence et autorité sur toutes les composantes de l'Organisation et sur toutes les régions du monde. Nous avons reçu un soutien indéfectible de la part de tous les membres du Conseil de l'ISO, avec une implication et un engagement accrus dans nos processus de gouvernance révisés. Une telle implication ne peut qu'être bénéfique à l'ISO.

L'engagement auprès des organisations internationales a été un élément décisif de notre travail. L'an dernier, en qualité de Président de l'ISO, j'ai pris l'engagement d'établir des passerelles encore plus solides avec notre organisation jumelle, la Commission électrotechnique internationale (IEC). Je suis enthousiaste et extrêmement heureux de noter l'intensification de la coopération et de la collaboration entre les deux organisations. Ce succès est dû en grande partie à l'énergie et au leadership de mon fidèle ami de longue date, le Président de l'IEC, Jim Shannon.

En ce qui concerne l'avenir, nous devrons accroître nos efforts pour soutenir le Programme de développement durable des Nations Unies à l'horizon 2030, conçu pour orienter notre monde sur une voie plus résiliente et plus prospère. Il est important pour nous d'utiliser judicieusement notre temps et d'agir de manière aussi décisive et rapide que possible. Il ne nous reste que 11 ans, notre engagement envers les Nations Unies doit être plus fort que jamais et nous continuerons à investir massivement pour aider le monde à atteindre les 17 Objectifs de développement durable.

Ces efforts ne sont qu'une partie – certes très importante – des activités que nous déployons face à l'ampleur des défis mondiaux. Pour ma part, la cybersécurité est ce qui m'inquiète le plus. C'est sans aucun doute l'une des préoccupations majeures du monde moderne. Si des cyber-activités perturbatrices et malveillantes sont à même de mettre fin ou de corrompre nos interconnexions mondiales, tous nos meilleurs processus et tous nos beaux efforts seront réduits à néant. La connectivité numérique joue un rôle central dans le renforcement de l'innovation et de la prospérité pour tous. Pourtant, dans notre avancée collective vers le progrès, l'augmentation des cybermenaces constitue un obstacle majeur et les gouvernements et l'industrie doivent, de toute urgence, renforcer les capacités dans ce domaine.

Fini le temps où les entreprises pouvaient s'en remettre à leur service informatique pour résoudre le casse-tête de la cybersécurité. La question est désormais un véritable enjeu de durabilité et de survie de l'entreprise. Les Normes internationales sont essentielles pour garantir la rigueur et l'efficacité des programmes de cybersécurité. Comme je l'ai déclaré aux dirigeants des gouvernements et de l'industrie dans le monde entier, l'ISO est particulièrement bien placée dans cette phase de transformation massive du cyberespace ; et nous établissons une collection de normes de premier ordre que les organisations peuvent intégrer dans leurs processus opérationnels quotidiens et dans leurs produits.

À l'aube de cette nouvelle année, nous ignorons ce qui nous attend en matière de cybersécurité. Que nous réservent les cybercriminels en 2019 ? Que devons-nous faire pour nous en protéger ? J'espère que ce numéro d'*ISOfocus* apportera quelques réponses à ces questions. Sur le terrain fragile de la cybersécurité d'aujourd'hui, les Normes internationales sont plus indispensables que jamais.

À titre très personnel, je pense que, dans le système de la normalisation internationale, c'est une obligation morale que de mettre de côté nos différences, de guérir nos petites rancœurs et d'épouser la mondialisation. L'isolement et la construction de murs entre nous conduira simplement à un échec institutionnel et environnemental massif, et finalement au désastre. En tant que membres de cette civilisation internationale, nous pouvons et nous devons nous attaquer de manière coopérative aux défis auxquels cette planète est confrontée. Qui peut vouloir que nos enfants héritent d'un monde incapable de survivre à cause de notre intérêt égoïste et de notre négligence ? Les normes ISO aident maintenant à aborder et à résoudre les défis mondiaux et nous devons veiller à ce qu'elles continuent à le faire à l'avenir. L'importance des enjeux est beaucoup trop élevée. ■

Nouveau changement en vue

#4thindustrialrevolution

CITATION Bertrand Piccard
Écoutez les propos de l'initiateur du projet Solar Impulse au sujet du rôle des normes dans le monde

Afin de souligner l'importance des normes pour la Quatrième révolution industrielle, l'ISO a mené, du 12 au 26 octobre 2018, une campagne mondiale sur ses plateformes de médias sociaux. Après le lancement avec la célébration de la Journée mondiale de la normalisation, l'accent a été mis sur la façon dont les normes ISO favorisant l'adoption de systèmes cyber-physiques seront utiles dans la vie quotidienne de chacun dans des domaines tels que la santé et la sécurité, les transports, la protection des données personnelles et les technologies bioscientifiques.

PLUS DE
3 300 000
IMPRESSIONS

CAMPAGNE
La campagne a réuni des membres de l'ISO, des parties prenantes et des experts du secteur pour débattre de la nécessité d'élaborer des normes qui faciliteront l'adoption continue des technologies émergentes dans notre vie quotidienne

PLUS DE
500 CONTRIBUTEURS
À NOTRE CAMPAGNE

THINGLINK Les Normes internationales et la Quatrième révolution industrielle
Aperçu de quelques comités techniques ISO

PLUS DE
1 700 000
UTILISATEURS JOINTS

VIDÉO Les normes et l'intelligence artificielle Partie 1
Entretien avec Wael William Diab, Président de l'ISO/IEC JTC 1/SC 42

VIDÉO Les normes et l'intelligence artificielle Partie 2
Entretien avec Wael William Diab, Président de l'ISO/IEC JTC 1/SC 42

PLUS DE
15 500
VISIONNAGES VIDÉO

VIDÉO Les normes et la chaîne de blocs
Entretien avec Philippa Ryan du groupe de travail ISO/TC 307/WG 3 sur les contrats intelligents (« smart contracts ») et leurs applications

ASSURER LA SÉCURITÉ INFORMATIQUE FACE AUX MENACES ACTUELLES

Photo : Kevin Ku/Unsplash

par Barnaby Lewis

Alors que la cybercriminalité pourrait engendrer USD 2 000 milliards de pertes annuelles d'ici à 2019 [1)] et qu'une multitude d'appareils mobiles et autres objets connectés vient chaque jour grossir la liste des cibles potentielles, il apparaît indispensable d'adopter une approche commune en matière de sécurité informatique.

La cybercriminalité offre d'alléchantes opportunités aux personnes mal intentionnées : enchevêtrement des réseaux, peines relativement légères, manque de cohérence dans la lutte contre le blanchiment d'argent, gains potentiels énormes… Pour se prémunir des attaques informatiques, les mots d'ordre sont préparation, détection des vulnérabilités et résilience au sein des systèmes globaux de management. C'est à ce niveau qu'intervient la norme ISO/IEC 27001 sur les systèmes de management de la sécurité de l'information (SMSI).

Fleuron de la famille ISO/IEC 27000, cette norme est le fruit du travail de l'ISO/IEC JTC 1, le comité technique mixte de l'ISO et de la Commission électrotechnique internationale (IEC) créé pour constituer un pôle de normalisation officielle des technologies de l'information. Depuis sa première version publiée il y a plus de 20 ans, elle a été constamment tenue à jour et élargie au point d'englober plus de 40 Normes internationales couvrant des aspects divers et variés, comme la création d'un vocabulaire commun (ISO/IEC 27000), la gestion des risques (ISO/IEC 27005), la sécurité dans l'informatique en nuage (ISO/IEC 27017 et ISO/IEC 27018) ou encore les techniques de criminalistique servant à l'analyse des preuves numériques et aux investigations sur incident (ISO/IEC 27042 et ISO/IEC 27043, respectivement).

En plus de faciliter la gestion de la sécurité de l'information, ces normes contribueront à l'identification des pirates informatiques, qui pourront alors être traduits en justice. Par exemple, ISO/IEC 27043 fournit des lignes directrices qui décrivent les processus et principes applicables à divers types d'investigations, y compris l'accès non autorisé, la corruption des données, les défaillances du système ou les violations de sécurité des informations d'entreprise, ainsi que toute autre investigation numérique.

1) Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", Forbes Online

Les mots d'ordre sont préparation et détection des vulnérabilités.

Garder une longueur d'avance

Le sous-comité SC 27 de l'ISO/IEC JTC 1, chargé des techniques de sécurité des technologies de l'information, a une responsabilité de taille : s'assurer que cette famille de normes continue de satisfaire les besoins en constante évolution des petites et grandes entreprises. C'est en grande partie grâce à la contribution de personnes comme le Professeur Edward Humphreys, qui préside le groupe de travail en charge de l'élaboration des SMSI, que celle-ci demeure l'un des outils de gestion des risques les plus efficaces face aux milliards d'attaques perpétrées chaque année [2)] contre des cibles inédites et selon des méthodes toujours plus sophistiquées.

2) Rapport ISTR (Internet Security Threat Report), Volume 23, Symantec, 2018

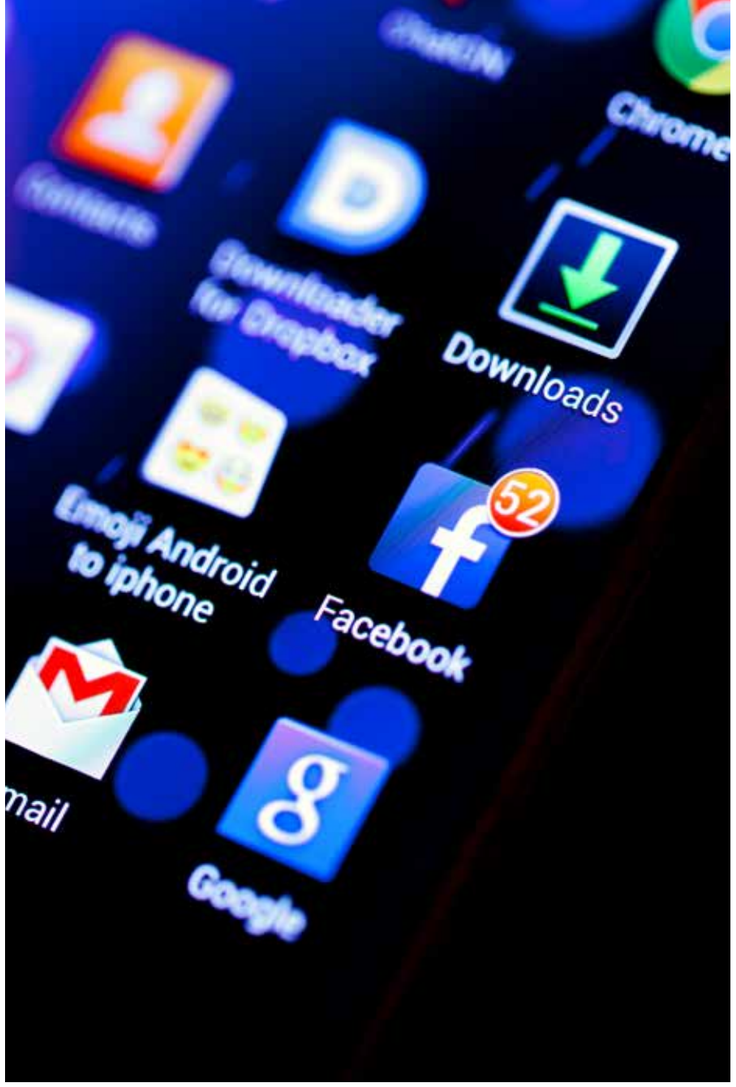
J'ai eu l'occasion de m'entretenir avec M. Humphreys, un spécialiste de la sécurité de l'information et de la gestion des risques fort de plus de 37 ans d'expérience dans les domaines du conseil et de l'enseignement supérieur, qui a d'abord répondu à la question fondamentale que tout le monde se pose sur les SMSI : comment ces systèmes peuvent-ils conserver une longueur d'avance sur les délinquants de façon à protéger les entreprises et les consommateurs ? « S'il est vrai que les risques qui pèsent sur l'information, les processus organisationnels, les applications et les services évoluent en permanence, ISO/IEC 27001 fait également l'objet d'une amélioration continue. Résultat : le processus intégré de gestion des risques permet aux entreprises de se tenir à jour dans leur lutte contre la cybercriminalité. »

Selon M. Humphreys, un organisme ainsi armé est en mesure d'évaluer les risques auxquels il est exposé, de mettre en place des mesures d'atténuation, puis d'assurer un processus de suivi et d'évaluation, et d'améliorer ainsi sa protection selon les besoins. De cette manière, il est toujours sur le qui-vive et préparé en cas d'attaque : « Utilisés correctement, les SMSI permettent de s'adapter au paysage changeant des cybermenaces. »

Derrière les menaces, des opportunités

À l'échelle d'une entreprise, la modélisation et l'atténuation des menaces sous toutes leurs formes représentent toujours une tâche colossale, qui impose d'utiliser un système de sécurité unifié et intégré. Or, compte tenu de la complexité des relations d'interdépendance, la question suivante se pose : les SMSI sont-ils une solution envisageable pour les petites et moyennes entreprises (PME) ? De l'avis de M. Humphreys, « les SMSI peuvent s'appliquer à tous les types d'organisation et à tous les modes de fonctionnement, y compris dans les PME. En tant que maillon des chaînes d'approvisionnement, elles doivent avoir la maîtrise et assurer la gestion de leur sécurité de l'information et des risques informatiques auxquels elles sont exposées, afin de garantir leur propre protection et celle d'autrui. » M. Humphreys explique en outre que les obligations d'une entreprise, comme le déploiement d'un SMSI, sont généralement définies dans des accords du niveau de service (à savoir des contrats conclus entre partenaires de la chaîne d'approvisionnement), en même temps que les besoins en matière de services et les responsabilités juridiques.

Le commerce en ligne présente indéniablement des défis pour les PME, mais ils sont largement compensés par l'énorme potentiel qu'offre l'Internet. Certaines personnes, à l'image d'Alan Wolff, Directeur général adjoint de l'Organisation mondiale du commerce, avancent d'ailleurs que les petites entreprises ont été les plus favorisées par l'avènement de la technologie. À l'occasion de l'Assemblée générale de l'ISO en 2018, ce dernier a en effet souligné que « quiconque a un projet, possède un ordinateur connecté à l'Internet et bénéficie de l'accès à une plateforme peut devenir un acteur à part entière du commerce international ».



> Notre vie privée est peut-être moins complexe que le monde des affaires, mais l'enjeu est tout aussi important.

Les avantages pour le développement socio-économique ne manquent pas, car l'Internet permet à un nombre croissant de personnes et de communautés auparavant isolées de jouer un rôle sur le marché mondial. Toutefois, il est indispensable de contrebalancer les inconvénients en adoptant une approche prudente et éprouvée comme celle fondée sur les SMSI. Et M. Humphreys de rappeler qu'« une cyberattaque visant un maillon de la chaîne d'approvisionnement peut perturber l'ensemble des acteurs » et avoir des répercussions bien au-delà de l'entreprise ciblée et de ses clients directs. Un constat qui se vérifie aussi bien pour les fabricants de jouets artisanaux de Bali que pour les services de santé publique nationaux en Europe.

Les deux enjeux : respect de la vie privée et climat de confiance

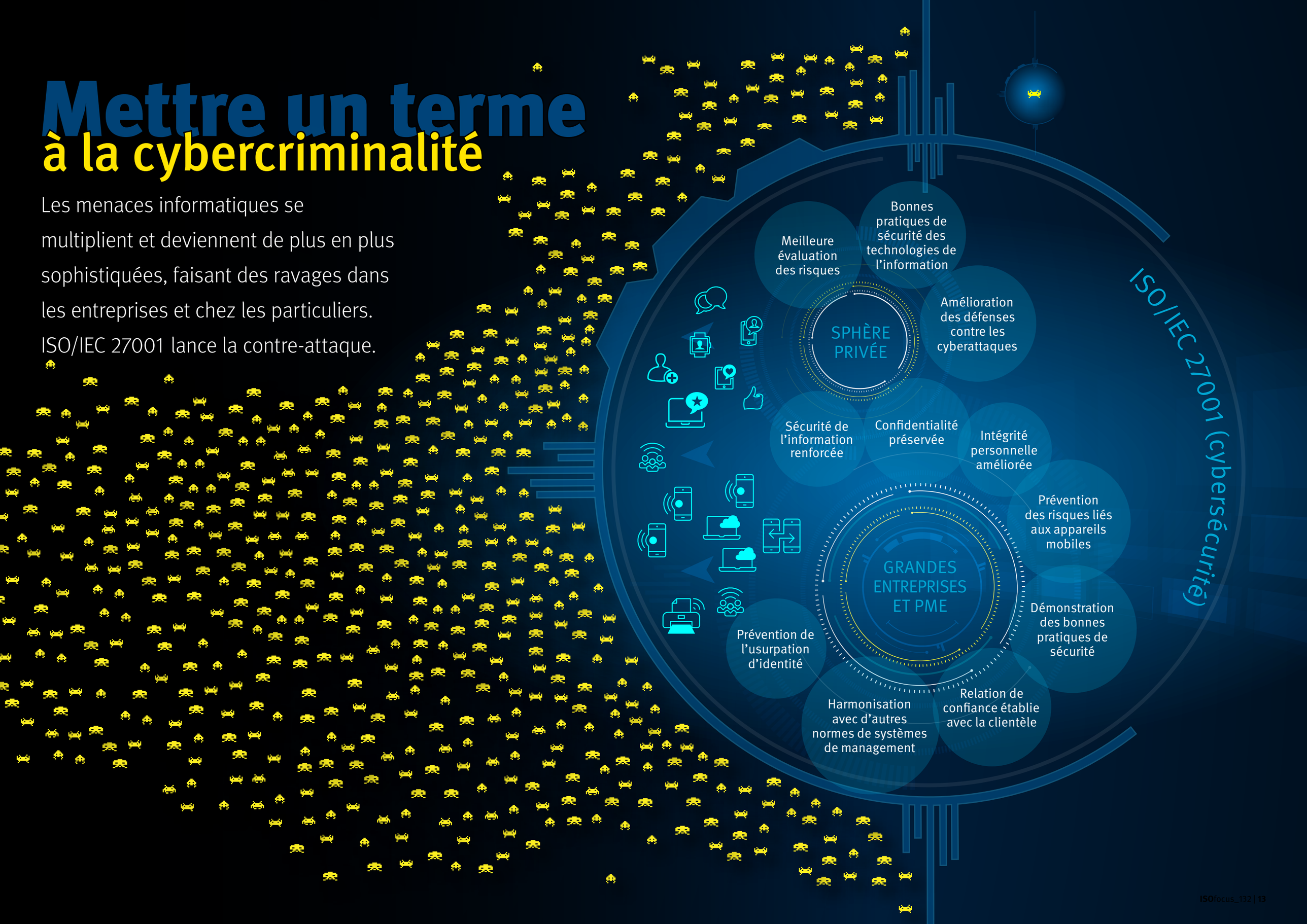
Notre vie privée est peut-être moins complexe que le monde des affaires, mais l'enjeu est tout aussi important. Pour beaucoup d'entre nous, le simple fait de recourir aux meilleures pratiques pour choisir un mot de passe et réaliser les mises à jour de sécurité (sans oublier de suivre notre intuition lorsqu'une affaire semble louche ou trop belle pour être vraie) devrait suffire à nous protéger des pirates informatiques la plupart du temps. On s'interroge cependant de plus en plus sur la façon dont les institutions et les entreprises stockent, analysent et monétisent les vastes quantités de données que nous leur fournissons plus ou moins volontairement.

J'ai demandé à M. Humphreys si, selon lui, la famille de normes ISO/IEC 27000 apporte des réponses à ces diverses inconnues : « Récemment, le sous-comité SC 27 a entrepris l'élaboration d'ISO/IEC 27552, une norme d'extension d'ISO/IEC 27001 visant à répondre aux besoins spécifiques en matière de protection de la vie privée. » Actuellement au stade de projet, ce document précise les exigences et formule les lignes directrices à suivre pour l'instauration, la mise en œuvre, le maintien et l'amélioration continue du management de la protection de la vie privée en entreprise.

Toute menace pesant sur la vie privée, les moyens financiers ou la réputation d'une personne ou d'une entreprise vient ébranler notre confiance et modifier notre comportement en ligne, mais aussi dans la vie réelle. La famille de normes ISO/IEC 27000 remplit alors une mission cruciale : nous permettre d'aller de l'avant. Si la numérisation toujours plus importante de notre vie a de quoi nous inquiéter, il est rassurant de savoir que l'on peut compter sur cette famille de normes régissant les systèmes de management de la sécurité de l'information et qu'un groupe mondial d'experts, comme celui dont fait partie M. Humphreys, est à pied d'œuvre pour nous donner toujours une longueur d'avance. ■

Mettre un terme à la cybercriminalité

Les menaces informatiques se multiplient et deviennent de plus en plus sophistiquées, faisant des ravages dans les entreprises et chez les particuliers. ISO/IEC 27001 lance la contre-attaque.



L'architecture *d'un futur connecté*

par Rick Gould

En 2018, l'ISO, en collaboration avec la Commission électrotechnique internationale (IEC), a publié la norme ISO/IEC 30141, toute première norme d'harmonisation établissant une architecture de référence pour l'Internet des objets (IoT) – assemblage complexe de milliards d'appareils intelligents connectés via l'Internet. L'application de la norme rendra l'IoT plus efficace, plus sûr, résilient et beaucoup plus sécurisé.

L'IoT est un réseau de dispositifs électroniques, souvent sans fil, qui permet de voir, de capter et même de contrôler une grande partie du monde qui nous entoure.

Abordé pour la première fois dans les colonnes d'*ISOfocus* en 2016, l'Internet des objet (IoT) a été, ces deux dernières années, un domaine riche en événements. Ce secteur en pleine expansion s'est doté d'un nouveau sous-comité entièrement consacré à l'élaboration de normes telles qu'ISO/IEC 30141, et plusieurs attaques fortement médiatisées ciblant l'IoT ont clairement démontré en quoi ces normes sont indispensables.

Voilà près de 20 ans, le Britannique Kevin Ashton, pionnier de la technologie RFID, qui travaillait chez Procter & Gamble, a inventé l'expression « Internet des objets » dans un exposé où il démontrait comment l'entreprise pouvait utiliser l'identification par radio-fréquence (RFID) – technique sans fil aujourd'hui largement appliquée dans les paiements sans contact et les cartes d'identification intelligentes – pour géolocaliser et suivre les produits. Et l'expression est restée.

La définition officielle de l'IoT formulée par l'ISO et la Commission électrotechnique internationale (IEC) est la suivante : « infrastructure d'entités, de personnes, de systèmes et de ressources d'information interconnectés avec des services qui traitent et réagissent aux informations du monde physique et du monde virtuel ». Mais en termes simples, l'IoT est un réseau de dispositifs électroniques, souvent sans fil, qui nous permet, et permet à des machines, de voir, de capter et même de contrôler une grande partie du monde qui nous entoure, que ce soit au niveau individuel ou à des échelles globales de plus grande ampleur.

En effet, les dispositifs et les systèmes IoT ont pris une place de plus en plus grande dans la plupart, sinon dans tous les aspects de la vie moderne. Certains sont déjà bien connus et entrés dans le langage courant sur les marchés des biens de consommation, mais les plus grands utilisateurs de l'IoT travaillent dans les secteurs de l'industrie, de la santé, de l'agriculture et des administrations. Pour faire simple, toute technologie qualifiée d'« intelligente » est susceptible de faire partie de la grande famille de l'IoT qui ne cesse de s'agrandir, avec, par exemple, les compteurs intelligents, les voitures intelligentes, les cartes intelligentes, les bracelets fitness intelligents, les villes intelligentes, les téléphones intelligents, les montres intelligentes, les services publics intelligents, l'agriculture intelligente, les soins de santé intelligents et même la fabrication intelligente, qui sera, on l'affirme, la prochaine révolution industrielle.

Nous rapprocher

Collectivement, l'IoT peut nous rendre plus connectés, mieux informés, plus efficaces et moins gaspilleurs. Mais s'il est mal utilisé, il peut affaiblir la sécurité et la résilience de nos réseaux informatiques et de nos données. Car c'est la relative simplicité des dispositifs de l'IoT qui est la source des problèmes mais aussi des opportunités. « Les avantages sont nombreux mais, dans le même temps, les plus grands risques pèsent sur la résilience et la sécurité » souligne François Coallier, Président du sous-comité SC 41, *Internet des objets et technologies connexes*, du comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*. L'ISO et l'IEC ont mis sur pied ce SC 41 chargé d'établir des normes pour l'IoT, au sein du JTC 1, qui traite quant à lui de la normalisation internationale dans le domaine des TI et a, depuis sa création en 1987, publié largement plus de trois mille normes.

Les défis que posent l'interopérabilité – c'est-à-dire la capacité des dispositifs de l'IoT de se connecter sans difficulté entre eux et avec d'autres systèmes – et la sécurité sont liés. « Les technologies évoluent sans cesse et à un rythme extrêmement rapide », ajoute Coallier, « de sorte que leur adjonction au réseau s'est effectuée à la fois rapidement et souvent au cas par cas, au fur et à mesure de l'émergence de nouvelles technologies. La croissance de l'IoT est exponentielle, et l'on estime que d'ici à 2020 le nombre de dispositifs IoT connectés pourrait atteindre les 50 milliards, avec un marché se chiffrant vraisemblablement en milliards de dollars.

UNE NUÉE D'AVANTAGES...

« Il existe déjà de nombreuses normes publiées en matière de résilience, de sûreté et de sécurité, mais ISO/IEC 30141 servira d'architecture de référence aux fins de leur application. »

François Coallier, Président de l'ISO/IEC JTC 1, *Technologies de l'information*, SC 41, *Internet des objets et technologies connexes.*

Une année frappante

2016, l'année où a été créé le JTC 1/SC 41, a également été une année frappante, au sens propre comme au figuré, pour l'Internet des objets, en raison d'attaques de grande ampleur sur les réseaux à travers l'IoT. En mars de cette année-là, par exemple, l'attaque du logiciel Mirai, qui a paralysé une grande partie de l'Internet dans l'Est des États-Unis, a été la plus grosse offensive sur l'Internet jamais réalisée. Beaucoup de gens ont été surpris de la rapidité de la propagation du code malveillant et de la facilité avec laquelle le pirate avait pu entrer dans des réseaux prétendument sécurisés. Alors, comment une telle frappe a-t-elle été possible ? En ciblant le maillon faible d'une chaîne ou, dans le cas précis, les dispositifs IoT à la périphérie du réseau.

« Les auteurs de la frappe ont ciblé notamment des dispositifs tels que les caméras de vidéosurveillance sans fil et les téléviseurs intelligents vendus avec un nombre limité de noms d'administrateur et de mots de passe par défaut », explique Coallier. Le fabricant a produit des millions de ces dispositifs. « Le botnet a essayé tour à tour chaque combinaison de nom d'administrateur et mot de passe jusqu'à ce qu'il trouve la bonne combinaison pour prendre le contrôle du dispositif » précise-t-il. « En parvenant à pirater plus d'une centaine de milliers de ces dispositifs, les pirates ont pu générer des attaques de déni de service à grande échelle qui ont mis temporairement à genou une partie du Web américain. »

Concernant un autre acte de piratage largement relayé dans les médias – une attaque d'ingénierie sociale sur les ordinateurs personnels (PC) de l'administration d'une usine ayant abouti à la paralysie de sa chaîne de production – Coallier précise, « dans ce cas, il semble qu'il ait été possible d'accéder aux systèmes de production de l'usine à partir de ces PC, ce qui n'aurait pas été le cas si les systèmes de production avaient été isolés des PC connectés à l'Internet par une segmentation adéquate du réseau. » Qui plus est, le réseau aurait pu être beaucoup plus sûr simplement en appliquant les processus et procédures bien documentés déjà décrits dans de nombreuses normes, telles que la série ISO/IEC 27033 pour les techniques de sécurité des TI, qui préconise la segmentation des réseaux pour une sécurité accrue.

Photo: Kaur Kristjan/Unsplash

Beaucoup de gens ont été surpris de la rapidité de la propagation du code malveillant et de la facilité avec laquelle le pirate avait pu entrer dans des réseaux prétendument sécurisés.

La même année que le botnet Mirai, un groupe de chercheurs israéliens a démontré comment il est possible de pirater un réseau d'éclairage, simplement à l'aide d'un drone aéroporté modifié, en exploitant la vulnérabilité d'une ampoule intelligente courante. En contournant les mesures de sécurité d'une seule et unique lampe, il est possible d'infecter les ampoules adjacentes compatibles et d'en prendre le contrôle. Selon ces chercheurs, s'il y a, dans une ville, suffisamment d'ampoules intelligentes utilisant les mêmes protocoles de communication, des attaquants malveillants peuvent facilement accéder et infecter en quelques minutes l'ensemble du réseau d'éclairage. Scénario extrême servant à démontrer la réalité des failles, l'exercice a montré le potentiel d'attaques malveillantes de grande ampleur dans des réseaux apparemment sécurisés, en exploitant des vulnérabilités négligées dans des dispositifs simples en périphérie du réseau.

Les normes de l'IoT

L'enjeu que posent les dispositifs IoT, c'est leur simplicité à laquelle vient se cumuler une mise en œuvre ad hoc involontaire, aggravée si les utilisateurs négligent la question de la sécurité. Bon nombre de ces dispositifs sont des mini-ordinateurs simplifiés, de faible puissance, avec un système d'exploitation compact fondé sur le système Linux largement disponible, que les pirates informatiques connaissent bien. Les dispositifs IoT ont des exigences différentes de celles des autres ordinateurs et lorsque les utilisateurs n'appliquent pas rigoureusement les normes en matière de sécurité, l'IoT devient une cible vulnérable. « Avec l'IoT, comme entre le yin et le yang, tout est une question d'équilibre. Les possibilités sont nombreuses, mais il est impératif de trouver le juste équilibre avec une mise en œuvre rigoureuse et d'accorder beaucoup plus d'attention à la sécurité », observe Coallier.

Les normes pour l'Internet des objets établissent un terrain d'entente.

C'est à ce niveau que les Normes internationales viennent soutenir l'opérabilité et la résilience de l'IoT. Comment peuvent-elles le faire ? La série de normes ISO/IEC 29192, par exemple, définit les techniques applicables en matière de cryptographie pour environnements contraints pour les appareils relativement simples, de faible puissance. Dans l'exemple de l'ampoule, les chercheurs israéliens ont recommandé une technique de sécurité spécifique décrite dans l'ISO/IEC 29192-5, qui spécifie trois fonctions de hachage adaptées aux applications nécessitant des implémentations cryptographiques en environnements contraints. Mais comme c'est le cas dans n'importe quel domaine en cours de développement, nous aurons aussi besoin de nouvelles normes, et c'est précisément le rôle du JTC 1/SC 41, dont le domaine des travaux couvre l'interopérabilité, la sûreté et, avant tout, la sécurité.

Ce sous-comité du JTC 1 a publié à ce jour 18 livrables, axés pour la plupart sur les réseaux de capteurs. Il a également publié des recommandations sous la forme d'un rapport technique ISO/IEC TR 22417, traitant des cas d'usage dans le domaine de l'Internet des objets (IoT), qui fournit un contexte pour les utilisateurs des normes de l'IoT. Ce document aborde des questions importantes telles que les exigences fondamentales, l'interopérabilité et les normes appliquées par les utilisateurs. Plus important encore, les exemples donnés précisent le rôle que les normes existantes ont à jouer et mettent en évidence les domaines où d'autres activités de normalisation sont nécessaires.

Établir les bases

Les normes pour l'Internet des objets établissent un terrain d'entente sur des sujets tels que la terminologie ou les architectures de référence, qui aideront les développeurs de produits à déployer un écosystème interopérable. L'ISO/IEC 30141 fournit une base et un cadre de référence pour les nombreuses normes applicables élaborées par le JTC 1/SC 41. « Il nous a paru utile de mettre en place une architecture de référence pour optimiser les avantages et réduire les risques », explique Coallier, qui préside le SC 41 du JTC 1. Autre norme fondamentale : ISO/IEC 20924, *Technologies de l'information – Internet des objets (IoT) – Définition et vocabulaire*. « Il est important que ceux qui travaillent sur l'IoT parlent le même langage », ajoute Coallier. ISO/IEC 20924 et ISO/IEC 30141 établissent ce langage indispensable.

Le groupe de travail qui a élaboré l'ISO/IEC 30141 a été dirigé par trois experts, notamment Jie Shen (Chine), lui-même appuyé par Wei Wei (Allemagne) et Östen Frånberg (Suède). Collectivement, ces chefs de projet comptent de nombreuses décennies d'expérience dans le domaine, et ont été soutenus par plus d'une cinquantaine d'autres spécialistes qui ont directement contribué à la norme. « L'IoT présente de nombreux risques et une foule d'opportunités », fait valoir Jie Shen, qui précise, « il nous faut mettre au point le mécanisme de mise à jour parfait pour surmonter ces risques ; c'est en soi un travail de détail très exigeant ».

MODÈLE D'ARCHITECTURE DE L'IoT S'ARTICULANT AUTOUR DE SIX DOMAINES
ISO/IEC 30141

Une grande partie de leurs travaux est déjà concrétisée dans les nombreuses normes publiées par les sous-comités du JTC 1, et la norme ISO/IEC 30141 établit une architecture de référence pour tous les fusionner, avec plusieurs nouvelles normes que le JTC 1/SC 41 est en train d'élaborer. « ISO/IEC 30141 fixe un cadre commun pour les concepteurs et les développeurs d'applications dans le secteur de l'IoT », explique Coallier. « La norme décrit les principales caractéristiques de l'IoT, ainsi qu'un modèle conceptuel et une architecture de référence », ajoute-t-il. De nombreux exemples accompagnent les descriptions.

Un modèle articulant six domaines

La norme ISO/IEC 30141 inclut également une structure inédite innovante pour l'architecture de référence de l'IoT, un modèle qui s'articule autour de six domaines. Ce modèle fournit un cadre pour les concepteurs de systèmes pour intégrer la multiplicité des dispositifs et des opérations dans l'IoT. L'équipe du projet a constaté que les approches conventionnelles ne sont pas applicables aux réseaux relativement simples. Comme l'explique Jie Shen : « Il est plus compliqué de construire l'écosystème dans l'IoT, pour relier de nombreuses entités hétérogènes telles que les utilisateurs humains, les objets physiques, les périphériques, les plateformes de service, les applications, les bases de données, les outils tiers et d'autres ressources. Nous avons compris que le modèle de référence conventionnel comportant différentes couches appliqué habituellement dans les systèmes informatiques était insuffisant. Le modèle à six domaines, pour sa part, peut aider à subdiviser très clairement l'écosystème de l'IoT et guider les utilisateurs à établir le nouveau modèle opérationnel de l'IoT. Le modèle lui-même sera encore plus efficace lorsqu'il est étayé par la technologie de la chaîne de blocs, la formule hautement sécurisée maintenant de plus en plus utilisée dans les transactions financières.

La norme traite également largement de l'interopérabilité – qui permet à divers types de dispositifs de communiquer sans discontinuité – et du concept de fiabilité de l'IoT, qui est défini comme le degré de confiance que des utilisateurs peuvent avoir qu'un système fonctionne comme prévu, tout en assurant la sécurité, la sûreté, la confidentialité, la fiabilité et la résilience face à des perturbations telles que les catastrophes naturelles, les défaillances, les erreurs humaines et les attaques. « De nombreuses normes ont déjà été publiées en matière de résilience, de sûreté et de sécurité, mais ISO/IEC 30141 fournit l'architecture de référence qui permet de les appliquer », souligne Coallier. Dans le même temps, étant donné que l'Internet des objets continue d'évoluer et de progresser, le JTC 1/SC 41 travaille actuellement à l'élaboration de neuf nouvelles normes pour l'IoT, afin d'assurer, avec des spécifications techniques, encore plus de fiabilité, d'interopérabilité et de sécurité. ■

LA cyber-confiance EN JEU

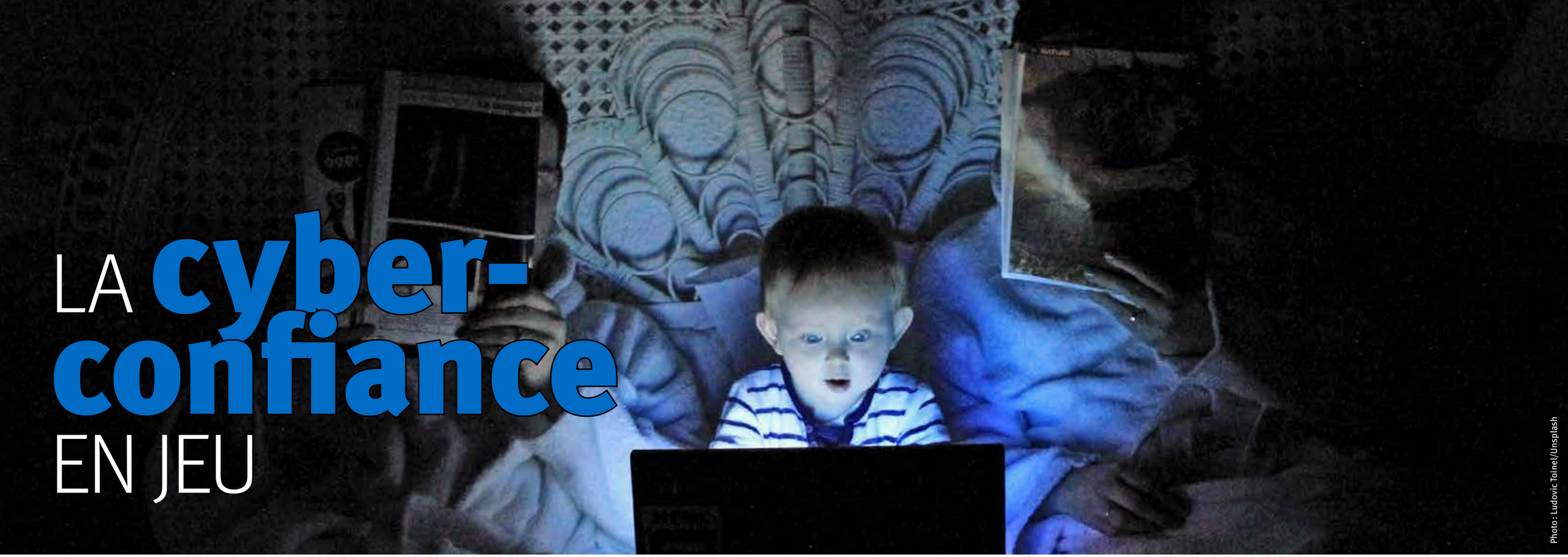


Photo: Ludovic Toinel/Unsplash

par Robert Bartram

Avec la sophistication constante des technologies qui offrent de meilleures opportunités mais présentent aussi de nouvelles vulnérabilités et menaces, différents types d'organisations risquent de donner prise à des attaques malveillantes ou à des violations de données à très grande échelle. La gestion des risques est donc tout aussi vitale dans le cyberespace que dans le monde physique. Quels sont donc ces cyber-risques ? Comment les Normes internationales peuvent-elles aider à les atténuer ? Est-il si sûr que la seule réponse soit celle d'un degré de sophistication encore plus élevé des technologies ?

Le Robert, dictionnaire de la langue française, définit le « risque », comme « un danger éventuel plus ou moins prévisible ». Pour obtenir des résultats, il faut prendre des risques, et ces risques doivent être bien gérés si l'on veut réussir et éviter des conséquences négatives.

Les risques sont impossibles à éviter. Il faut les assumer, cela fait inévitablement partie de la vie, à la fois personnelle et professionnelle, de tout un chacun. En effet, quel que soit le secteur de l'industrie dans lequel elle exerce dans ce monde hautement compétitif d'aujourd'hui, si une entreprise ou une organisation ose prétendre qu'il n'y a aucun risque dans ses activités – proclamant ainsi une absence totale de risque –, non contente de manquer à ses obligations statutaires et légales, elle fera très rapidement faillite et disparaîtra.

Pourtant le risque peut aussi être une force de progrès. Une bonne gestion des risques peut déboucher sur des résultats très positifs et, pour atteindre leurs objectifs, les entreprises doivent prendre des risques. Avant de prendre des décisions stratégiques importantes, les organisations ont besoin d'un peu de certitude et il est essentiel de comprendre que le risque est effectivement l'incidence probable de l'incertitude sur ces décisions. En bref, l'enjeu en matière de risque concerne la gestion des décisions dans un monde déjà complexe, volatil et ambigu, et qui le devient rapidement de plus en plus.

La menace numérique

Cet enjeu est particulièrement vrai en matière de cyberrisque. Dans le cyberespace, lorsqu'il s'agit d'aborder les questions de sécurité au niveau national ou au niveau de l'entreprise, le degré d'incertitude est à chaque fois très élevé. La menace ne tient pas au contexte et aux circonstances du marché, elle vient d'« acteurs malveillants » qui cherchent à lancer des offensives criminelles. Invisibles, ces cyberattaquants sont comme les fantômes et les revenants des légendes populaires, et leur invisibilité ne fait qu'exacerber le sentiment de menace, car ils cherchent à nuire, ont la capacité de le faire, sont agiles et savent s'adapter.

De jour en jour, pour ne pas dire d'heure en heure, la technologie gagne en sophistication. Autrefois, la criminalité industrielle portait par exemple sur le vol de documents laissés négligemment sur un bureau, mais l'ampleur du méfait se limitait au maximum au contenu d'un attaché-case. Maintenant, avec une clé USB ou des techniques d'exfiltration, le même criminel numérique peut s'emparer de giga-octets d'informations dont l'équivalent papier représenterait le contenu d'une pile de valises si haute qu'elle pourrait toucher la lune. Cela ne tient pas seulement au fait que – du papier au numérique – la sophistication du stockage des données a progressé de manière hyper-exponentielle, mais au fait que la nature et l'objectif des données ont aussi changé. Un criminel qui veut mettre la main sur des produits médicaux protégés, par exemple, n'a plus besoin d'entrer par effraction dans un local de stockage, il peut en copier les données au format numérique et cloner le produit avec une imprimante 3D.

Il est absolument évident que les organisations de tout type ont besoin d'une « cyber protection » d'une forme ou d'une autre. Et de surcroît, elles ont également besoin d'un système suffisamment robuste pour les prévenir de toute attaque – réelle ou supposée – aussi rapidement que possible. Dans le cyberespace, il y a deux catégories de menaces : les menaces internes et les menaces externes. Pour concevoir et mettre en place avec succès un système de protection contre les menaces venant de l'extérieur, il faut être attentif aux intentions et aux capacités des éventuels acteurs externes malveillants – établir ce qu'ils recherchent, leur mobile, et les technologies dont ils disposent.

Les organisations doivent se préparer aussi aux menaces de malveillants internes et d'acteurs qui, en interne, ont par imprudence laissé le système vulnérable à d'éventuelles attaques. La négligence dans l'utilisation de données personnelles peut exposer un individu au chantage et au dévoiement par une organisation mal intentionnée. Les organisations peuvent avoir les meilleurs pare-feu du monde, ils ne serviront à rien face à un acteur interne détenteur de niveaux d'accès élevés, capable de voler des informations sans être détecté.

De jour en jour, pour ne pas dire d'heure en heure, la technologie gagne en sophistication.

Ce qui compte vraiment

Alors, comment les gouvernements, les entreprises et les individus se protègent-ils face à de telles menaces ? Le comité technique ISO/TC 262, *Management du risque*, a élaboré la norme ISO 31000 sur le management du risque, qui crée un cadre de principes et de processus pour la gestion des risques en général. Jason Brown, qui est le Président de ce TC, a été, entre autres, chargé de la gestion de l'évaluation et de l'assurance de la cybersécurité au Département australien de la défense. Il explique que, comme pour toute gestion des risques, une organisation qui entend se protéger sérieusement contre les cyber-risques, doit « revenir aux objectifs qu'elle poursuit et se focaliser sur le cœur de ses activités en s'attachant à ce qui compte vraiment, autrement dit bien cerner son capital le plus précieux ».

Les entreprises et les gouvernements doivent évaluer avec soin la valeur et la nature de ce qui leur tient à cœur. Par exemple, si une organisation est gardienne de propriétés intellectuelles techniques de haut niveau sous forme de données, la fuite ou le vol de ces données aura des conséquences dramatiques, conséquences qui seront encore plus dommageables si les données en question sont détenues pour le compte d'autres personnes qui dépendent de cette organisation dans une chaîne logistique, car une brèche dans le système risque d'entraîner la rupture de toute la chaîne. Ce qui compte en premier lieu, c'est donc une vue d'ensemble stratégique du système, et non une évaluation de la technologie proprement dite.

Sur le moteur de recherche de Google, le nombre de résultats pour « ISO 31000 » en 0,54 seconde dépasse les 6,5 millions.

Cette approche fait écho à celle de Donald R. Deutsch, Vice-président et Responsable Normes chez Oracle, en Californie, et Président du sous-comité SC 38, *Plateformes et services d'applications distribuées*, du comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, un groupe d'experts travaillant sous la houlette conjointe de l'ISO et de l'IEC (Commission électrotechnique internationale). Le nuage, et sa position dans la hiérarchie du risque, a peut-être la plus grande importance immédiate pour les consommateurs quotidiens. De nos jours, si nous utilisons un ordinateur, il est très probable que nous allons également utiliser le nuage. Mais l'« informatique en nuage », observe M. Deutsch, « est davantage une stratégie de déploiement et d'affaires qu'une stratégie technologique ». Il y a certainement des améliorations technologiques récentes avec des risques inhérents – comme le provisionnement automatique des ressources de calcul qui sont partagées par plusieurs utilisateurs –, pourtant « les risques sont très semblables à ceux de n'importe quel environnement informatique, mais exacerbés et amplifiés en raison de leur échelle ».

Le prix de la résilience

Les Normes internationales étayent cette approche stratégique du cyber-risque. Comme le souligne Jason Brown, lorsqu'il s'agit d'aborder les cyber-risques, il convient de prendre en compte la série ISO 31000 en même temps que la série ISO/IEC 27000 sur les systèmes de management de la sécurité de l'information (SMSI). Une telle approche met en balance la technologie et les « facteurs humains ». La famille de normes ISO/IEC 27000 aide une organisation à évaluer ses besoins purement technologiques, tandis qu'ISO 31000 l'aide à comprendre la valeur des informations ou des produits qu'elle détient dans le cyberespace, et donc le degré de protection technologique dont elle a besoin pour prévenir les attaques. Pour dire les choses autrement : grâce à une évaluation approfondie des risques à l'aide d'ISO 31000, une organisation quelle qu'elle soit peut s'épargner des dépenses substantielles s'agissant de l'acquisition de sécurité technologique. Une mauvaise évaluation des risques peut tout aussi bien conduire à ne pas payer assez ou à payer trop cher un système de protection.

Ces deux séries de normes ne sont en aucun cas les seules qui peuvent aider à atténuer les risques cybernétiques. La cybersécurité doit également être examinée en termes de continuité d'activité, et la série ISO 22301 relative à la gestion de la continuité d'activité y pourvoit. Cette série vise la mise en place d'un « système de management documenté afin de se protéger des incidents perturbateurs [...] lorsqu'ils surviennent ». Elle permet à une organisation d'évaluer comment son système d'information et de télécommunications soutient ses objectifs et quelles en seraient les conséquences s'il flanchait. L'investissement d'une organisation dans la cybersécurité peut être dicté par le niveau de dépendance au système ; une petite organisation peut être en mesure de continuer à se servir (voire à réutiliser le cas échéant) des pièces justificatives sur papier, tandis qu'un géant comme Amazon dépend littéralement de la connectivité.

De même, les travaux de l'ISO/IEC JTC 1/SC 38 aident les producteurs – et donc en définitive les consommateurs – à parler un langage commun pour l'informatique en nuage. Or, ici, et c'est très important, ce ne sont pas, comme c'est généralement le cas, les producteurs ou les vendeurs eux-mêmes qui ont sollicité l'élaboration de cette série de normes, mais les clients et les acheteurs. En effet, les gouvernements et la société civile ont fait valoir que, chaque producteur utilisant sa propre terminologie, il était impossible de comparer les produits et d'opérer des choix en toute connaissance de cause. C'est cette demande qui a abouti à la publication d'ISO/IEC 17789, *Technologies de l'information – Informatique en nuage – Architecture de référence*, qui établit une architecture de référence et un cadre de vocabulaire commun. Le sous-comité SC 38 a également supervisé l'élaboration d'ISO/IEC 19086, une norme en quatre parties, dont deux encore en cours d'élaboration, sur les accords du niveau de service entre les fournisseurs de nuage et leurs clients.

L'informatique en nuage est davantage une stratégie de déploiement et d'affaires qu'une stratégie technologique.

CYBERSÉCURITÉ
FAITS ET CHIFFRES

92 %
des logiciels malveillants sont encore transmis par e-mail

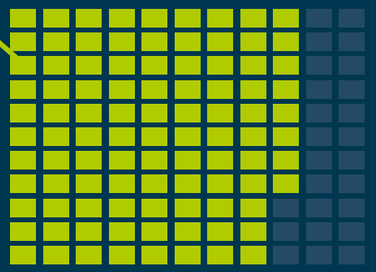
VULNÉRABILITÉ DES SYSTÈMES DE COMMANDE INDUSTRIELS

54%
DES ENTREPRISES INTERROGÉES ONT SUBI UN INCIDENT DE SÉCURITÉ RELATIF À LEUR SYSTÈME DE COMMANDE INDUSTRIEL AU COURS DES 12 DERNIERS MOIS

16%
ONT ENREGISTRÉ AU MOINS TROIS INCIDENTS

ATTAQUES RÉUSSIES EN 2017

77 %
d'attaques sans fichier



Source : Principaux faits, chiffres et statistiques pour 2018 en matière de cybersécurité
www.csoonline.com

Une progression fulgurante

L'impact positif de toutes ces normes sur la cybersécurité en général et sur les cyberrisques en particulier est indéniable. La norme ISO 31000 a été adoptée par une quarantaine de pays comme système national de gestion des risques. Du reste, sur le moteur de recherche de Google, le nombre de résultats pour « ISO 31000 » en 0,54 seconde dépasse les 6,5 millions.

Les technologies évoluent à un rythme toujours plus rapide et les Normes internationales doivent rester en phase. Les outils qui fonctionnent aujourd'hui ne fonctionneront peut-être pas demain. Par exemple, du fait que l'apprentissage automatique évolue vers l'intelligence artificielle, il se peut que le système intègre en matière d'apprentissage à la fois des capacités d'ordre adaptatif et « philosophique » qui n'existent tout simplement pas dans le monde d'aujourd'hui. Les capacités d'analyse des données se développent à tel point que de grandes quantités de données peuvent être analysées pour repérer les questions émergentes qui ne seraient pas détectables autrement. L'avènement de l'informatique quantique augmentera aussi exponentiellement la vitesse de l'informatique. La conjonction de ces trois changements dans le cybermonde sera « probablement la plus grande révolution que nous ayons connue depuis la découverte de l'électricité ou de l'atome », dit Jason Brown. Cela ne prend même pas en compte les nanotechnologies ou l'interconnectivité croissante de tous les objets.

Lorsque ces facteurs finiront par se combiner, l'environnement concurrentiel pour se démarquer en affaires, entre pays, entre rivaux et avec l'adversaire le plus redouté, sera nettement plus rapide. Tant et si bien que nous continuerons certainement encore d'établir le risque en termes d'objectifs, mais notre capacité réelle à faire face au cyberespace sera peut-être négligeable. L'ISO/TC 262 s'attelle actuellement au domaine du « management des risques émergents », en mettant l'accent sur les risques susceptibles d'engendrer les plus graves perturbations. Comme l'indique clairement M. Brown, les consommateurs et les producteurs doivent aborder l'avenir différemment, et nous devrons tous « être beaucoup plus ouverts à ce monde très volatil et très ambigu ». ■

Une plateforme de *performance*

ISO/IEC 27001 (sécurité de l'information)

ISO/IEC 29192-1 (cryptographie pour environnements contraints)

ISO/IEC 27002 (management de la sécurité de l'information)

ISO/IEC JTC 1/SC 27
Techniques de sécurité des technologies de l'information

ISO/IEC 27042 (analyse des preuves numériques)

ISO/IEC 27032 (renforcement de la cybersécurité)

Famille ISO/IEC 27033 (sécurité de réseau)

ISO/IEC 27043 (investigations sur incident)

ISO/IEC 27005 (gestion des risques liés à la cybersécurité)

Future ISO/IEC 27552 (exigences de protection de la vie privée)

ISO/TC 262
Management du risque

ISO 31000 (management du risque pour les organisations)

Future ISO 31050 (management des risques émergents)

ISO/IEC 31010 (techniques d'évaluation des risques)

Future ISO 31030 (management des risques en déplacement)

Future ISO 31022 (management des risques juridiques)

Future ISO/IEC 20924 (vocabulaire de l'Internet des objets)

ISO/IEC 30141 (architecture de référence de l'Internet des objets)

Future ISO/IEC 30149 (cadre de confiance de l'Internet des objets)

ISO/IEC JTC 1/SC 41,
Internet des objets et technologies connexes

ISO/IEC TR* 22417 (cas d'utilisation de l'Internet des objets)

ISO/IEC 27035 (préparation à la continuité d'activité)

Famille ISO/IEC 27035 (réponse aux cyberattaques)

ISO/TC 292
Sécurité et résilience

ISO/IEC 27017 (contrôles de sécurité de l'information pour l'informatique en nuage)

ISO/IEC 19944 (utilisation des données dans les services en nuage)

Famille ISO 22301 (management de la continuité d'activité)

ISO/IEC 27018 (protection des informations personnelles dans l'informatique en nuage public)

ISO/IEC JTC 1/SC 38
Plateformes et services d'applications distribuées

ISO/IEC 20933 (systèmes d'accès)

Famille ISO/IEC 19086 (cadre de travail de l'accord du niveau de service)

ISO/IEC 17789 (architecture de référence pour l'informatique en nuage)

* TR : rapport technique

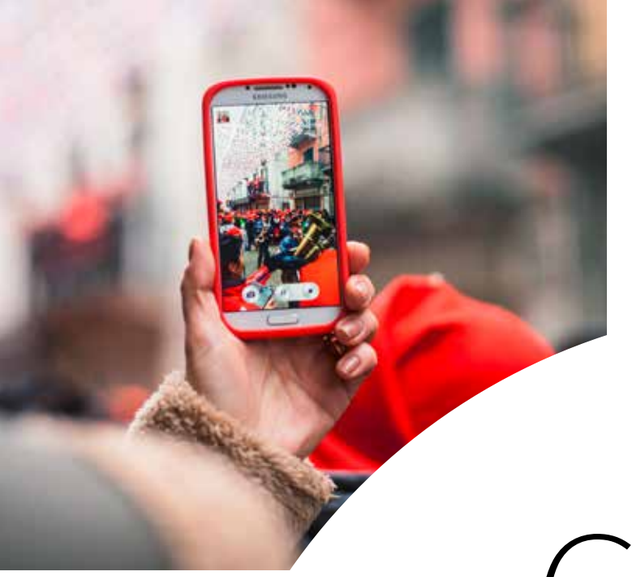


Photo : Hal Gatewood/Unsplash

Ces 5 choses-là aussi peuvent être piratées !

Photo : James Hicks/Unsplash

par Elizabeth Gasiorowski-Denis et Vivienne Rojas

Les objets qui font notre quotidien sont de plus en plus connectés, ce qui nous facilite grandement la vie, ainsi que celle des pirates informatiques. Prendre conscience des dangers liés à ces dispositifs en réseau est le premier pas à accomplir pour écarter les intrus.

Les cyberattaquants s'en prennent aussi aux nourrissons. Comment peuvent-ils s'immiscer dans une chambre de bébé ? Des lieux aussi sacro-saints que les chambres d'enfants sont désormais la cible de pirates informatiques malintentionnés, à l'affût à l'extérieur de vos foyers. Aujourd'hui, il faut le savoir, si les cybercriminels peuvent prendre le contrôle de votre babyphone, c'est que tous les objets « connectés » peuvent être attaqués, et c'est là que le bât blesse.

Gartner Inc. prévoit que d'ici à 2020, 20,4 milliards d'objets connectés seront utilisés dans le monde. Le segment grand public en est le plus gros utilisateur, avec 5,2 milliards d'objets connectés en 2017, soit 63% du nombre total des applications en service. Nombreux sont déjà les foyers équipés de plus d'une dizaine d'appareils connectés : ordinateurs, téléphones portables et tablettes, mais aussi d'équipements électroménagers plus classiques, tels que réfrigérateurs, téléviseurs et systèmes de sécurité.
Au travers d'une étude sur la vulnérabilité des dispositifs de l'Internet des objets, des chercheurs de l'Université Ben Gourion de Beer-Sheva (Israël) ont découvert que de nombreux fabricants et propriétaires de dispositifs facilitaient en fait le travail des pirates. En effet, bon nombre des fabricants utilisent le même mot de passe par défaut pour tous les appareils d'un même type et, souvent, les utilisateurs ne prennent pas la peine de le modifier. La conséquence est simple : si vous avez dix appareils connectés sur un réseau, la sécurité de l'ensemble du réseau est compromise si un seul de ces appareils est laissé sans surveillance. Effrayant, non ?
À dire vrai, pratiquement tous les appareils qui sont reliés à une connexion Wi-Fi stable peuvent être piratés ou contrôlés par un pirate « professionnel ». Sauf s'il n'est pas directement connecté à l'Internet, un dispositif peut, d'une manière ou d'une autre, être la cible d'une attaque. L'éventail des objets concernés est très large. Examinons ici cinq exemples de ces objets qui peuvent être piratés.

Babyphones et caméras de surveillance

À quoi sert un babyphone ? À surveiller de jeunes enfants. Voilà précisément pourquoi l'appareil représente une telle menace lorsqu'il est piraté et/ou exploité. Les bébés, et même les jeunes enfants, peuvent être observés à distance par quiconque parvient à prendre le contrôle de l'appareil. Semblablement, pour permettre de voir ce qui s'y passe

Pratiquement tous les appareils qui sont reliés à une connexion Wi-Fi stable peuvent être piratés ou contrôlés par un pirate « professionnel ».

quand nous ne sommes pas chez nous, bon nombre de caméras de sécurité sont aujourd'hui connectées à l'Internet. À la suite d'incidents largement rapportés dans les médias concernant des babyphones piratés par des personnes malveillantes, le Service de protection des consommateurs de New York a émis une mise en garde du public quant à la sécurité de ces appareils.

Imprimantes et télécopieurs

Dans les maisons ou les bureaux, il est fréquent que les imprimantes aient leur propre connexion Internet pour communiquer, souvent sans fil, avec d'autres dispositifs. Pour les pirates, cette connexion constitue le point d'entrée qui leur permet d'accéder à distance au réseau. Il leur suffit de contourner les éventuels contrôles de sécurité pour s'introduire dans une imprimante ou d'autres appareils connectés. La vulnérabilité des imprimantes a été clairement démontrée, un pirate ayant même affirmé s'être introduit dans 150 000 imprimantes pour sensibiliser l'opinion à cet égard.
Les pirates peuvent même infiltrer votre réseau en envoyant un simple fax. La plupart des télécopieurs étant aujourd'hui intégrés à des imprimantes multifonctions connectées à un réseau Wi-Fi et à une ligne téléphonique, ils peuvent être facilement piratés avec un fichier image bien conçu contenant un code malveillant. Lorsque ce code est converti en données à transmettre sur le réseau informatique interne, il peut prendre le contrôle du télécopieur et voler des mots de passe et des coordonnées bancaires, puis pirater d'autres appareils connectés au réseau.

Photo : Hal Gatewood / Unsplash

Des commerçants ont été forcés de retirer de la vente un certain nombre de jouets « connectés » ou « intelligents » après que des failles de sécurité eurent été découvertes.

Jouets

Oui, cet adorable ours en peluche connecté est un terrain de jeu pour les cybercriminels. Apparemment, dès qu'un dispositif est connecté à l'Internet, il est piratable. Cela vaut aussi pour de nombreux appareils et objets que l'on n'associe pas d'ordinaire à une technologie de ce type, notamment les jouets. Tout jouet connecté à l'Internet avec un micro, une caméra ou un système de géolocalisation est un risque pour la vie privée ou la sécurité des enfants. Qu'il s'agisse de poupées parlantes ou de tablettes conçues pour les enfants, des commerçants ont été forcés de retirer de la vente un certain nombre de jouets « connectés » ou « intelligents » après que des failles de sécurité permettant à un étranger de parler à l'enfant ou d'écouter ses conversations eurent été découvertes dans les protocoles Bluetooth et Wi-Fi. Dans chacun de ces jouets, la connexion Bluetooth n'avait pas été sécurisée, autrement dit, le pirate n'avait pas besoin de mot de passe, de code ni d'autre moyen d'authentification pour obtenir l'accès.

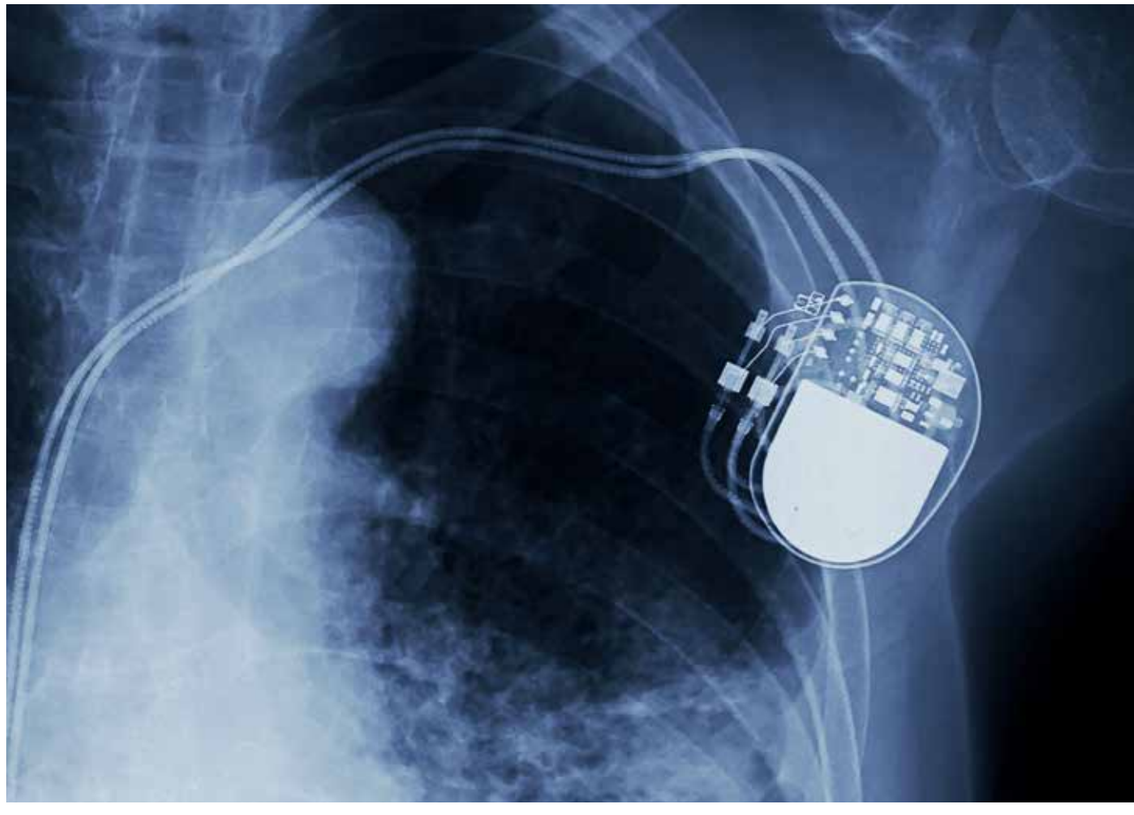
Appareils intelligents

En matière de sécurité, votre réfrigérateur est peut-être votre pire ennemi ! Cet appareil qui vous permet d'envoyer directement vos listes de courses à votre smartphone peut être connecté d'une façon qui permet la récupération des identifiants de connexion à Google. Ainsi, tout dispositif ou appareil domestique qui est connecté peut devenir une porte d'entrée à l'ensemble du réseau. S'il est pratique de pouvoir régler à distance la température de votre logement, par exemple pour augmenter le chauffage au moment où vous quittez le bureau, sachez qu'un pirate peut fort bien prendre le contrôle du thermostat et le bloquer jusqu'à ce que vous payiez une rançon. Autre cible de choix des cybercriminels : les machines à café. Une faille de sécurité dans l'application mobile qui permet de commander votre cafetière à distance peut ouvrir la voie à une violation de vos données privées si un pirate dérobe votre mot de passe Wi-Fi et exfiltre toutes les données qui transitent sur votre réseau.

Aux États-Unis, la Food and Drug Administration a fait rappeler 465 000 stimulateurs cardiaques menacés d'un piratage potentiel.

Stimulateurs cardiaques et implants

Votre cœur peut être piraté et ce n'est pas une plaisanterie ! En 2017, aux États-Unis, la Food and Drug Administration (FDA) a fait rappeler 465 000 stimulateurs cardiaques menacés d'un piratage potentiel à cause d'une vulnérabilité informatique permettant à un cybercriminel d'influencer le rythme cardiaque du patient et, possiblement, d'en provoquer la mort. Et que dire de la stimulation cérébrale profonde, qui consiste à implanter des électrodes dans le cerveau, pour aider à maîtriser les tremblements des patients atteints d'épilepsie ou de la maladie de Parkinson. Cette prise de contrôle précise du cerveau ouvre aux pirates la possibilité d'aller encore plus loin dans la malveillance que la commande des pompes à insuline ou des implants cardiaques. La prise de contrôle de l'implant électronique cérébral d'une personne (appelée « brainjacking ») par un cybercriminel peut entraîner la perturbation de l'appareil moteur, altérer l'autonomie de la personne, en modifier les émotions ou l'affect, induire des douleurs et une modulation du système de récompense. Se pose alors la question suivante : si les implants cérébraux sans fil se généralisent, comment pourra-t-on assurer l'accès exclusif des médecins et écarter tout risque de cybercriminalité ?



LE SAVIEZ-VOUS ?

Si vous avez dix appareils connectés sur un réseau, votre sécurité peut être compromise si un seul de ces appareils est laissé sans surveillance.

Le segment grand public en est le plus gros utilisateur, avec 5,2 milliards d'objets connectés en 2017.

Préserver la sécurité

Les pirates peuvent user de bien d'autres stratagèmes apparemment tout aussi improbables pour pénétrer dans votre système. Même avec une porte d'entrée principale à l'Internet bien protégée, quelqu'un pourrait réussir à pénétrer en catimini. Que faut-il donc en conclure pour notre avenir ? Doit-on s'inquiéter que tous ces objets intelligents tissent leur Toile ? La réponse est oui, et pour cause ! Nous ne sommes pas en 2020 et pourtant les failles de sécurité sont déjà légion.

Il est urgent de protéger notre cyberespace, cette question exige une attention immédiate et constante. Souvent, il suffit de prendre les bonnes mesures de sécurité pour décourager les pirates les plus zélés et vaincre les opportunistes, et souvent les Normes internationales sont notre première ligne de défense. Des normes telles qu'ISO/IEC 27001 ou ISO/IEC 27002 proposent un langage commun pour traiter des questions de gouvernance, de risques et de conformité liées à la sécurité des données, tandis que les normes ISO/IEC 27031 et ISO/IEC 27035 aident les organisations à réagir efficacement aux attaques informatiques, à les diffuser et à s'en remettre. Il existe également de nombreuses autres normes qui définissent les mécanismes de cryptage et de signature électronique pouvant être intégrés dans des produits et des applications pour protéger les transactions en ligne, l'utilisation des cartes de crédit et les données stockées.

Mais les normes n'ont un intérêt que dans la mesure où elles sont appliquées. Alors, la prochaine fois que vous achèterez un babyphone ou tout autre dispositif connecté, posez-vous les bonnes questions. Le fabriquant a-t-il envisagé l'éventualité d'un piratage ? L'entreprise a-t-elle mis en œuvre les Normes internationales appropriées ? Si la réponse à ces deux questions est non, vous devriez peut-être y réfléchir à deux fois. ■

SOIXANTE ANNÉES DE
SÉCURITÉ INCENDIE

Lors de sa réunion plénière annuelle 2018, le comité technique ISO/TC 92, *Sécurité au feu*, a célébré son 60e anniversaire, l'occasion d'une rétrospective de six décennies de production de normes acceptées au niveau international sur les essais au feu, le mesurage des paramètres d'incendie, l'ingénierie de la sécurité incendie et d'autres sujets connexes. Cette réunion, qui s'est tenue en octobre dernier à Delft, aux Pays-Bas, était hébergée par le NEN, membre de l'ISO pour ce pays. L'organisme de normalisation néerlandais a été félicité pour l'organisation exceptionnelle de l'événement et pour les chocolats et petits fours préparés tout spécialement pour marquer cet anniversaire.


Photo : NEN

Les délégués de l'ISO/TC 92 devant le « Het Meisjeshuis » à Delft, un ancien orphelinat de filles qui, après rénovation, a réouvert ses portes au printemps 2005 comme lieu de rencontre culturel.

Les festivités se sont terminées par un dîner de gala en présence de Mme Marja van Bijsterveldt, Bourgmestre de Delft, qui a prononcé une allocution enthousiaste dans laquelle elle a largement fait référence aux normes ISO, soulignant l'importance de la normalisation dans les efforts visant à renforcer la sécurité incendie. Patrick van Hees, Président de l'ISO/TC 92, s'est ensuite vu décerner un certificat de mérite par Rik van Terwisga, Directeur du NEN, pour marquer ce jalon important.

Au milieu de ces célébrations, les travaux de normalisation n'ont toutefois pas été oubliés et l'ISO/TC 92 et ses quatre sous-comités ont accompli des progrès considérables dans leurs différents domaines de compétence. Au cours des réunions, le comité a examiné la possibilité d'étendre ses activités à de nouveaux secteurs comme les grands feux de plein air, les tunnels et les constructions souterraines, ainsi que la santé et la sécurité des sapeurs-pompiers – signe manifeste que ce comité est là pour durer.

L'ISO/TC 92 souhaite remercier Efectis, FTT-Fire Testing Technology, Kingspan, Etex Group et DGMR d'avoir parrainé ces réunions.

PRÉSENTATION DES NORMES ISO
LORS DU FORUM MONDIAL DE L'INVESTISSEMENT

Pour plus d'informations :

http://worldinvestmentforum.unctad.org/iso

À l'occasion du dernier Forum mondial de l'investissement de la CNUCED qui s'est déroulé à Genève, en Suisse, l'ISO s'est associée à des acteurs mondiaux de l'innovation, des banques de développement, des parties prenantes du secteur privé et des représentants de premier plan des pouvoirs publics et de l'industrie pour mettre l'accent sur l'importance des normes ISO.

Plus de 80 participants ont assisté à la séance d'information sur le thème « Les normes ISO pour contribuer à mener à bien le Programme 2030 », dont l'objectif était de mettre en avant la contribution des normes à la réalisation des Objectifs de développement durable (ODD), le Programme de développement durable des Nations Unies visant à promouvoir la paix et la prospérité à l'horizon 2030. Cet événement, qui proposait un programme interactif comprenant des tables rondes et des discussions, a également permis aux participants d'échanger leurs expériences sur des thèmes tels que le commerce international ou encore sur les défis liés aux politiques publiques. Les Normes internationales constituent des outils efficaces pour les organisations et les entreprises désireuses de relever le défi des ODD.

La séance de l'ISO figurait parmi quelque 60 événements, dont trois sommets, cinq tables rondes ministérielles, des discussions dirigées par le secteur privé et des cérémonies de remise de prix. L'objectif commun du Forum, organisé tous les deux ans par la CNUCED, est de renforcer la coopération transfrontalière afin de promouvoir les investissements internationaux en tant que moteurs de la croissance économique et du développement.

LANCEMENT D'ISO 55002
SUR LA GESTION D'ACTIFS

La nouvelle édition d'ISO 55002 a été officiellement lancée à Amersfoort, Pays-Bas, par le comité technique ISO/TC 251, dont le domaine des travaux concerne la gestion des ressources. Ce lancement a été officialisé lorsque Rhys Davies, Président du comité, et Ton van Wingerden, Animateur, ont symboliquement remis le premier exemplaire de la norme à Anton van der Sanden, Directeur de Royal HaskoningDHV NL, société néerlandaise de conseil en ingénierie qui, pendant une semaine, accueillait à son siège social la réunion de l'ISO/TC 251, chargé d'élaborer la suite de normes ISO 55000 sur les systèmes de gestion d'actifs.

Composante essentielle de la série, ISO 55002 fournit des lignes directrices pour la mise en œuvre d'un système de gestion d'actifs, conformément aux exigences d'ISO 55001. Cette révision majeure, fondée sur les retours d'information et d'expérience de ceux qui ont d'emblée utilisé la norme, contient des préconisations sur la création d'un plan stratégique de gestion d'actifs, le traitement du risque dans la gestion d'actifs et l'application d'ISO 55001 dans des organismes de toutes tailles. Mis au point par un groupe d'experts internationaux originaires de 30 pays, dont la plupart ont joué un rôle déterminant dans l'élaboration d'ISO 55001, c'est un document de poids qui reste fidèle à l'esprit des exigences initiales tout en capitalisant sur les enseignements apportés par les retours d'information à l'échelle mondiale.

Publiée pour la première fois en 2014, la suite de normes ISO 55000 compte trois normes dont la pertinence et la popularité ne sont plus à démontrer. À propos de ce succès, Rhys Davies observe qu'ISO 55000 explique « pourquoi » un organisme a besoin d'un système de gestion d'actifs, ISO 55001 indique « quoi » faire pour se conformer à la norme et ISO 55002 donne des lignes directrices précisant « comment » procéder pour respecter les exigences de la norme. M. Davies est convaincu que la mise à jour d'ISO 55002 favorisera significativement l'adoption, dans le monde entier, de ce système de gestion.


Photo : NEN

Rhys Davies (à droite), *Président du comité ISO/TC 251, et* ***Ton van Wingerden*** (à gauche)*, Animateur, remettent le premier exemplaire d'ISO 55002:2018 à* ***Anton van der Sanden,*** *Directeur de Royal HaskoningDHV NL.*

LES PHILIPPINES
SOUS LE SIGNE DE LA NORMALISATION

Sergio Mujica, Secrétaire général de l'ISO, s'est rendu au Bureau of Philippine Standards (BPS), membre de l'ISO pour les Philippines, à l'occasion de la célébration, à Manille, de la Semaine nationale annuelle des normes. Organisée de façon à coïncider avec la Journée mondiale de la normalisation, qui se tient chaque année le 14 octobre pour rendre hommage aux travaux effectués en collaboration par les experts du monde entier qui élaborent les Normes internationales, la semaine a débuté par un concours d'essais sur les normes et un concours d'affiches auxquels ont participé quelque 150 élèves du secondaire scolarisés dans des établissements de la capitale philippine et des environs.

Dans un exposé instructif, Sergio Mujica a donné une vue d'ensemble de l'histoire de l'ISO et de son système de normalisation, en mettant en avant les nombreux avantages que les normes apportent aux pouvoirs publics, à l'économie et aux consommateurs, ainsi que leur impact constructif sur les avancées technologiques. Évoquant le faible niveau de participation des Philippines aux programmes de normalisation de l'ISO, imputable au manque de ressources, il a terminé son allocution en adressant aux collégiens un message fort pour les encourager à devenir les professionnels de la normalisation de demain.

Lors de sa visite de deux jours à Manille, le Secrétaire général de l'ISO a rencontré des membres du Congrès philippin, ainsi que des professionnels de la normalisation réputés, afin d'examiner la question de la mise en place d'une infrastructure qualité nationale, une proposition vivement soutenue par le BPS qui contribuerait au développement économique du pays.


Photo : BPS

Le Secrétaire général de l'ISO, ***Sergio Mujica,*** *prend un selfie avec un groupe de collégiens à Manille.*

POUR DES TOILETTES **DIGNES**

« Les Normes internationales sont essentielles pour l'essor de nouvelles technologies dans le domaine de l'assainissement et pour le développement d'une filière qui permet de sauver des vies », a déclaré le Secrétaire général de l'ISO, Sergio Mujica, lors du Salon des toilettes réinventées (Reinvented Toilet Expo) qui s'est tenu en octobre dernier à Beijing, en Chine. Le Secrétaire général a pris la parole lors d'une table ronde de haut niveau, à laquelle ont également participé Bill Gates, co-Président de la Fondation Bill et Melinda Gates, et Jim Yong Kim, Président de la Banque mondiale, ainsi que d'autres représentants gouvernementaux et de l'industrie de premier plan.

Soutenu par la fondation Gates, ce sommet d'une durée de trois jours a permis d'examiner les perspectives mondiales de l'assainissement autonome, un système d'assainissement permettant de traiter de façon sûre les déchets sans qu'il soit nécessaire de les raccorder à un réseau d'égouts classique. La gamme des systèmes présentés lors de ce salon était extrêmement diversifiée, avec des toilettes à traitement biologique et chimique ou dotées de membranes de filtration des liquides, conçues pour qu'un plus grand nombre de personnes vivant dans des régions en développement puisse se soulager en toute sécurité et dans la dignité.

Une évolution de cette ampleur n'est pas une tâche facile, mais la technologie peut désormais s'appuyer sur une nouvelle Norme internationale traitant des systèmes d'assainissement autonomes. En établissant des exigences de performance et de sécurité pour les unités de traitement intégrées, ISO 30500 permettra non seulement de fabriquer ces systèmes de façon efficace, mais aussi de développer le secteur dans son ensemble, garantissant ainsi à des milliards de personnes l'accès à un système d'assainissement sûr, indispensable pour une vie productive en pleine santé.

***Bill Gates** met en avant l'intérêt des nouveaux systèmes pour les sanitaires en se présentant sur scène avec un bocal rempli d'excréments humains.*

ÉLARGISSEMENT DE LA COOPÉRATION ISO/AOAC

L'ISO et l'AOAC INTERNATIONAL (AOAC) ont annoncé en 2018 le renouvellement de leur accord de coopération pour l'élaboration et l'approbation conjointes de normes et de méthodes communes. Signé pour la première fois en 2012 pour une durée de cinq ans, ce partenariat de haut niveau avec l'AOAC, organisme scientifique international à but non lucratif qui se consacre à la production de méthodes d'analyse chimique fiables, vise à accroître significativement la pertinence mondiale de ces deux organisations, grâce à l'adoption de normes communes approuvées par le Codex Alimentarius.

Dans le cadre de cet accord renouvelé, l'AOAC et l'ISO peuvent participer à leurs travaux réciproques, et s'engager dans l'élaboration commune de normes au travers de groupes de travail réunissant des experts de l'AOAC et de l'ISO. Ces travaux, soumis au processus d'approbation parallèle de l'AOAC et de l'ISO, déboucheront sur des normes qui seront ensuite publiées par les deux organisations.

Cette coopération axée à l'origine sur le lait et les produits laitiers va étendre son champ d'action pour inclure les projets relevant du domaine des travaux du comité technique ISO/TC 34, *Produits alimentaires*. Les priorités futures en matière de normes AOAC/ISO concerneront peut-être davantage de travaux sur l'analyse de la teneur en éléments nutritifs, et s'étendront aux contaminants, aux adultérants et aux résidus de pesticides, dans l'intérêt de l'ensemble des parties prenantes de l'industrie agroalimentaire.

PARTENARIAT DE L'ISO AVEC LE GROUPE DE LA BANQUE MONDIALE

POUR AIDER LES PAYS À FACILITER LE COMMERCE

L'ISO a établi un partenariat avec le Groupe de la Banque mondiale pour aider, selon leurs besoins, les membres de l'ISO dans les pays en développement à mettre en œuvre l'Accord sur la facilitation des échanges (AFE) de l'Organisation mondiale du commerce (OMC). Le partenariat couvrira des domaines tels que l'application des bonnes pratiques visant à éviter les obstacles techniques au commerce et s'attachera, en particulier, à la mise en œuvre de procédures d'évaluation de la conformité.

L'accord de partenariat a été établi lors d'un atelier sur la coopération entre organismes de contrôle aux frontières, qui s'est déroulé du 14 au 16 novembre 2018 au Cap, Afrique du Sud, où l'ISO était invitée à présenter un exposé sur « Les normes et la facilitation des échanges ».

Organisé par le Groupe de la Banque mondiale, le Secrétariat de l'OMC, le Secrétariat de la Convention internationale pour la protection des végétaux (CIPV), l'Organisation mondiale de la santé animale (OIE), l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO) et l'Organisation mondiale des douanes (OMD), cet atelier a réuni des hauts responsables de 12 pays africains engagés dans la mise en œuvre de l'AFE, afin de leur permettre de partager leurs expériences et d'apprendre les uns des autres.

Le Programme d'appui à la facilitation des échanges du Groupe de la Banque mondiale soutient activement les pays en développement pour qu'ils alignent leurs lois, procédures et processus relatifs à la facilitation des échanges en vue de la mise en œuvre de l'AFE.

Dans la plupart des pays en développement, le membre de l'ISO, l'organisme national de normalisation (ONN), est le Point d'information national défini dans l'Accord de l'OMC sur les Obstacles techniques au commerce et il arrive qu'il fournisse également des services d'évaluation de la conformité.

L'ISO s'est également engagée, lors de l'atelier, à fournir au Groupe de la Banque mondiale des informations sur les outils associés à l'AFE dont elle dispose concernant les activités des ONN.

PORTER LES PRIORITÉS MONDIALES

– CALENDRIER 2019

Les Objectifs de développement durable (ODD) des Nations Unies offrent une vision d'un monde plus juste, plus prospère, d'un monde pacifique et durable. Grâce à son expertise et ses ressources, l'ISO est idéalement positionnée pour soutenir ses membres dans la réalisation des ODD, qui ont chacun un lien avec les travaux de l'ISO.

Découvrez comment les normes ISO contribuent aux 17 ODD en téléchargeant le Calendrier ISO 2019. Sur 17 mois, vous pourrez y voir quelques-unes des nombreuses façons montrant comment l'ISO peut aider à mener à bien le Programme 2030, pour ne laisser personne de côté.

Le Calendrier ISO 2019 peut maintenant être téléchargé sur iso.org.

ISO/IEC 20000-1: **faciliter le parcours des données**

Photo : Markus Spiske/Unsplash

Les données, tout comme le Cloud qui les héberge, possèdent une valeur quasiment illimitée pour les organisations qui savent comment les traiter, à condition de mettre en place une stratégie adéquate pour libérer tout leur potentiel. Orange Business Services aide ses clients à transformer leurs données en actifs à part entière, en bénéficiant de l'appui de l'ISO/IEC et de sa norme de gestion des services informatiques.

À l'ère de la révolution numérique, les organisations produisent des données comme jamais. Telles quelles, ces données ne sont ni plus ni moins qu'une simple matière première. Cependant, les organisations qui parviennent à les transformer en renseignements utiles peuvent bénéficier d'une infinité de nouvelles possibilités. Grâce au Cloud Computing, elles peuvent accéder à des fonctionnalités informatiques performantes, et disposent d'un degré de flexibilité inédit pour l'externalisation de tout ou partie de leurs systèmes d'information, espaces de travail, serveurs, applications et solutions de stockage.

Le Cloud existe depuis un peu plus d'une décennie, mais son adoption continue à se heurter à un obstacle majeur : les préoccupations relatives à la sécurité et à l'intégrité des données. Dans ce contexte, les intégrateurs de systèmes à même de proposer des solutions de contrôle d'accès et de sécurité hébergées dans le Cloud (et donc d'offrir à leurs clients un vaste éventail de services gérés à distance tout en dynamisant la valeur globale de l'entreprise) seront parfaitement armés pour l'avenir.

Orange Business Services en fait partie. Fournisseur mondial de technologies de l'information et de la communication (TIC), la branche B2B du groupe Orange, lequel compte 260 millions de clients répartis dans 28 pays et réalise un chiffre d'affaires annuel de EUR 41 milliards, se veut un acteur de pointe dans ce que l'on appelle le « parcours des données ». Avec son expertise en matière de collecte, de transfert, de sécurité, de stockage, de traitement, d'analyse et de partage de données, mais aussi de création de valeur, Orange Business Services soutient les organisations à toutes les étapes de leur transformation digitale. Apporter son assistance à une si grande échelle implique qu'Orange Business Services pilote des processus homogènes au niveau mondial et les gère dans le cadre d'un modèle de gouvernance d'entreprise applicable dans le monde entier.

Pour cette entreprise, la mise en œuvre d'ISO/IEC 20000-1, *Technologies de l'information – Gestion des services – Partie 1 : Exigences du système de management des services*, s'est donc imposée comme un objectif logique. Élaborée conjointement par l'ISO et la Commission électrotechnique internationale (IEC), cette norme phare de la famille ISO/IEC 20000 aide les organisations à intégrer une stratégie de cycle de vie des services dans leur fonctionnement, en leur fournissant de meilleures pratiques sur la manière de gérer leur portefeuille de services afin qu'il reste à jour. Avec la publication en 2018 d'une nouvelle édition améliorée, nous étions curieux de savoir comment l'entreprise allait pouvoir maintenir son engagement à offrir des services complets de qualité à ses clients du monde entier. Nous avons interrogé à ce propos Jean-Pierre Girardin, de la division Services Clients & Opérations chez Orange Business Services.

***ISOfocus* : Quelles sont les raisons qui expliquent l'engouement d'Orange Business Services pour la norme ISO/IEC 20000-1 ?**

Jean-Pierre Girardin : Avec une clientèle de plus de trois mille multinationales renommées à l'échelon mondial, et de plus de deux millions de professionnels, d'entreprises et de collectivités locales en France, Orange Business Services s'appuie largement sur les normes relatives à la sécurité de l'information. D'ailleurs, nous sommes certifiés ISO/IEC 20000-1 depuis dix ans.

Dès le départ, nous avons pris la décision, en toute connaissance de cause, d'instaurer cette norme selon un schéma progressif et intégré. Nous avons donc conçu nos systèmes d'entreprise initiaux de management de la qualité à partir d'ISO 9001, de façon à optimiser nos processus de management des services dans un cadre fondé sur l'intégration. Ainsi, nous avons pu harmoniser nos processus sur l'ensemble des sites d'exploitation d'Orange Business Services à travers le monde.

Pour une société de services B2B, l'obtention de la certification ISO/IEC 20000-1 était à l'époque une opportunité en or. En plus d'optimiser nos services, elle nous a permis de bénéficier de l'association vertueuse de trois normes de systèmes de management : ISO 9001 (qualité), ISO/IEC 20000-1 (services informatiques) et ISO/IEC 27001[1] (sécurité de l'information), ainsi que des boucles d'amélioration continue inhérentes à ces normes.

1) ISO/IEC 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*, a été élaborée conjointement par l'ISO et la Commission électrotechnique internationale (IEC).

Quels sont les principaux avantages d'ISO/IEC 20000-1 pour Orange Business Services ?

La mise en œuvre d'ISO/IEC 20000-1 s'est accompagnée d'un certain nombre d'avantages clés, aussi bien en interne qu'en externe. Notre triple certification, renouvelée tous les ans avec un élargissement régulier de son domaine d'application, place Orange Business Services en position de partenaire de confiance et représente une véritable reconnaissance de la qualité de notre système de management au niveau mondial. Depuis, nous avons instauré ISO 14001 en sus pour le management environnemental sur trois de nos sites. Tous nos indicateurs attestent que la satisfaction client a significativement augmenté suite à cette démarche. En outre, le programme de certification s'est révélé un excellent moyen de renforcer la cohésion de nos équipes et de constituer une base solide grâce à laquelle nous avons pu poursuivre sur cette lancée au fil des ans.

L'engouement croissant autour d'ISO/IEC 20000-1 n'est pas surprenant si on le rapporte aux préoccupations actuelles en matière de sécurité. Pouvez-vous nous expliquer en quoi cette norme apporte une plus-value ?

ISO/IEC 27001, qui concerne la sécurité de l'information, recouvre un domaine d'application précis de nos activités et de nos entités (opérations, services Cloud…). C'est donc le paragraphe 6.6 d'ISO/IEC 20000-1 sur le management de la sécurité de l'information qui nous a aidés à sécuriser l'étendue de nos processus et activités sur trois niveaux : exigences de service, contrôles de sécurité des opérations et mise en place d'un portefeuille de services de sécurité gérés.
Par exemple, nous effectuons une surveillance proactive des incidents risquant d'affecter les actifs qui nous sont confiés et intervenons lorsqu'ils se produisent. Pour y parvenir, nous veillons à ce que toutes les modifications fassent l'objet d'une évaluation préalablement à leur mise en œuvre, afin d'empêcher toute atteinte à la protection des données. Nous avons également mis en place des contrôles de sécurité robustes qui se sont avérés très efficaces dans le cadre de nos processus et procédures de travail.
Les éléments de sécurité supplémentaires d'ISO/IEC 20000-1 contribuent également à sensibiliser les effectifs sur le fait que la sécurité doit faire partie intégrante des pratiques opérationnelles. D'ailleurs, des auditeurs ont reconnu le comportement exemplaire de nos équipes en matière de protection de l'intégrité des données.

Dans quelle mesure ISO/IEC 20000-1 est-elle intégrée dans les processus, les opérations et la stratégie d'Orange Business Services ?

Depuis le démarrage du projet en 2008, la norme ISO/IEC 20000-1 est totalement intégrée dans notre système de management de la sécurité, qui est mondialement cohérent. Cette intégration a revêtu une grande importance, car elle a coïncidé avec la certification ISO/IEC 27001 de notre centre d'assistance client (Major Service Center, MSC) au Caire en Égypte, suivie de celle du MSC de Gurgaon près de Delhi en Inde, et, pour finir, la certification de nos centres implantés en France, au Brésil et à l'île Maurice. Tout cela signifie que les exigences d'ISO/IEC 20000-1 imprègnent l'ensemble de nos processus et activités, qu'il s'agisse des relations avec les clients, des activités avec les fournisseurs ou encore du cycle de vie des services, de la commande à la livraison.
Au niveau stratégique, Orange Business Services mène des revues de direction régulières à l'échelle locale, régionale et mondiale, où nos résultats en matière de certification sont suivis attentivement. Nous anticipons les attentes de nos clients et réajustons le domaine d'application selon la direction prise par l'activité.

Votre réussite dans la mise en œuvre d'ISO/IEC 20000-1, principalement par des ressources internes, est impressionnante. Avez-vous des astuces à partager avec nos lecteurs d'*ISOfocus* ?

Lorsque l'on s'engage sur la voie de la certification, il est important de ne pas brûler les étapes. Nous avons commencé par former une équipe spécialisée, informée et qualifiée pour gérer le projet. À cet effet, une parfaite maîtrise du cadre ITIL, qui contribue à harmoniser les services informatiques avec les besoins métier, était pour nous un véritable atout. En outre, nous avons estimé qu'il était important d'effectuer une analyse méthodique des lacunes ainsi qu'une étude de faisabilité avant de lancer la certification d'un nouveau service. Nous avons également renforcé notre groupe d'auditeurs internes pour valider nos avancées au moyen d'audits annuels de l'ensemble de nos processus et entités.
Par ailleurs, pour susciter l'adhésion de nos effectifs à ce projet, nous avons organisé des séances de sensibilisation sur ISO/IEC 20000-1, et tous les aspects liés à la certification et à la normalisation. Fidèles à notre approche pragmatique, nous avons tenu à communiquer sur les avantages d'un parcours de certification, notre but étant que tout le monde comprenne pourquoi nous mettions en œuvre cette norme. L'enjeu n'était pas tant d'expliquer dans le détail les aspects techniques, mais plutôt de montrer comment les clients, les services et les processus allaient en bénéficier. Cette stratégie a bien entendu été entérinée par la direction, ce qui a été un élément déterminant pour la réussite du programme.

Une nouvelle version d'ISO/IEC 20000-1 a récemment été publiée. Avez-vous quelques pistes de réflexion sur la marche à suivre ? Des projets ou des plans pour l'avenir ?

La nouvelle version d'ISO/IEC 20000-1 ouvre des perspectives passionnantes pour Orange Business Services. Elle est harmonisée avec la nouvelle structure-cadre (HLS) utilisée pour toutes les normes de systèmes de management ISO, dont font partie ISO 9001:2015, ISO/IEC 27001:2013 et ISO 14001:2015. Cette version actualisée sera donc encore plus facile à comprendre.
Chez Orange Business Services, nous réfléchissons déjà à la façon de nous adapter aux changements, notre ambition étant de figurer parmi les premières entreprises à mettre en œuvre avec succès la nouvelle édition. C'est le défi qui nous attend en 2019 ! ■

Photo : Orange Business Services


Photo : Orange Business Services

***Jean-Pierre Girardin**, Services Clients & Opérations chez Orange Business Services.*

Grâce au Cloud Computing, les organisations peuvent accéder à des fonctionnalités informatiques performantes.