

Cybersécurité, un des piliers de la stabilité des entreprises
C'est l'une des nombreuses préoccupations du chef d'entreprise.

Perspectives

Septembre 2026

« *La cybersécurité par les Dirigeants, par les Chefs d'entreprise* »



Cybersécurité, un des piliers de la stabilité des entreprises

— Par Perpétus Jacques Hounbo

Neal Jetton, directeur de la Cybercriminalité à INTERPOL, a déclaré à propos des cybercriminels : « Ces organisations cybercriminelles infligent des dommages financiers et psychologiques dévastateurs à des particuliers, des entreprises et des communautés entières avec leurs fausses promesses¹ ». En tant que dirigeant et chef d'entreprise, vous devez au minimum prémunir votre entreprise contre ces dommages.

Stabilité pour asseoir croissance et rentabilité

Croissance et rentabilité sont des préoccupations que les chefs d'entreprise inscrivent à juste titre en tête de leurs priorités. Ces deux concepts traduisent et éclairent la raison d'être de l'entreprise. Il existe déjà de nombreux obstacles (surcharge administrative, micro-management, manque de délégation, etc.) qui peuvent empêcher le chef d'entreprise de se concentrer sur la croissance et la rentabilité de son entreprise. Lorsqu'en plus les capacités du chef d'entreprise sont absorbées par des dommages créés par des incidents de cybersécurité, le péril pour l'entreprise est encore plus grand. La cybersécurité est un accélérateur de confiance et un bouclier pour protéger ses actifs.

En vue d'aider le dirigeant d'entreprise à la prise en compte complète de cet accélérateur de confiance, le Forum Économique de Davos a édité en octobre 2019 "*Le guide de la cybersécurité pour les dirigeants dans le monde numérique d'aujourd'hui*". Je n'ai pas la prétention de m'adresser aux dirigeants qui participent à Davos, je m'adresse à tous ceux qui ont des responsabilités au niveau de PME/PMI, aux dirigeants de startups, aux nombreuses petites mains qui font vivre les grosses machines des grandes banques par exemple. Ce guide de la cybersécurité énonce un ensemble de 10 principes qui, à mon avis, s'appliquent aussi à ces petites unités auxquelles je faisais tantôt référence.

Il existe de nombreuses normes, de nombreux cadres organisationnels et processuels pour assister le dirigeant d'entreprise dans cette responsabilité. La norme ISO 27001 en est une. Le détail des ressources de la norme ISO 27001 sera présenté ultérieurement.

<https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2026/Une-operation-d-envergure-menee-en-Afrique-contre-les-escroqueries-en-ligne-donne-lieu-a-651-arrestations-et-permet-de-recuperer-4-3-millions-d-USD>

10 Principes de cybersécurité pour les leaders

Pour l'heure, en partant du guide élaboré par le Forum Économique de Davos, énumérons juste ces principes ci-dessous :

Principe n° 1 : Adopter la mentalité d'un dirigeant d'entreprise

Le dirigeant d'entreprise a aussi pour responsabilité de sensibiliser le conseil d'administration et la direction générale à l'importance de la gestion des risques cybernétiques. Il lui incombe de veiller à ce que la cybersécurité soit considérée comme un élément essentiel de la stratégie et de la réussite de son entreprise.

Principe n° 2 : Favoriser les partenariats internes et externes

Au sein de l'entreprise, la cybersécurité est par essence une affaire d'équipe : dirigeants, responsables informatiques, responsables juridiques et de la protection de la vie privée, etc. Au-delà de la mise en place de ces équipes en interne, il devient de plus en plus important de s'associer à des organisations externes afin de partager des informations sur des questions liées à la sécurité, telles que les menaces et les bonnes pratiques.

Principe n° 3 : Mettre en place et appliquer des pratiques rigoureuses en matière de cybersécurité

Toute entreprise doit pour le moins veiller à la mise en place de bonnes pratiques de cybersécurité.

Principe n° 4 : Protéger l'accès aux actifs essentiels à la mission

Il est primordial pour une entreprise d'adopter des stratégies et des technologies innovantes, adaptées à ses besoins. La mise en place d'un système solide de gestion des identités et des accès en fait partie.

Principe n° 5 : Protéger le domaine de messagerie contre le phishing

Le courrier électronique est, de nos jours, l'un des moyens de communication les plus précieux et les plus répandus, et la plupart des organisations en dépendent fortement. Le protocole Internet sur lequel repose le courrier électronique (SMTP) a été conçu il y a près de 45 ans³ sans tenir compte des aspects de sécurité; il est aujourd'hui vulnérable à un large éventail d'attaques. Le courrier électronique constitue le point d'entrée le plus courant : en moyenne, une entreprise reçoit plus de 90 % des logiciels malveillants détectés par ce canal. Il est crucial de réduire le risque d'utilisation abusive des e-mails en mettant en œuvre un ensemble de mesures appropriées.

Principe n° 6 : Adopter une approche « Zero Trust » pour sécuriser la chaîne d'approvisionnement

Le dirigeant d'entreprise qui ne fait pas procéder régulièrement à une évaluation du niveau de risque cybernétique présenté par ses fournisseurs de matériel et de logiciels devrait se rappeler que les pirates informatiques, eux, font systématiquement ces évaluations et exploitent toute faille qu'ils découvrent. Une approche « zéro confiance » en matière de sécurisation de la chaîne d'approvisionnement doit devenir la norme.

Principe n° 7 : Prévenir, surveiller et réagir face aux cybermenaces

Étant donné que la question n'est pas de savoir si un incident se produira, mais quand il se produira, une entreprise doit surveiller les cybermenaces

³ <https://www.rfc-editor.org/info/rfc821/>

tant en interne qu'en externe, et tester régulièrement les systèmes critiques et exposés à Internet afin d'en détecter les failles. De plus, elle devra surveiller Internet, les réseaux sociaux et le dark web à la recherche de données volées et d'informations sur les principaux dirigeants et les opérations commerciales, susceptibles d'être utilisées à des fins d'ingénierie sociale, d'attaques de spearphishing et de campagnes d'escroquerie. La manière dont une entreprise gère cette situation inévitable revêt une importance cruciale.

Principe n° 8 : Élaborer et mettre en pratique un plan global de gestion de crise

La gestion de crise est un élément essentiel de tout programme de sécurité dans le monde actuel, où la question n'est pas de savoir « si » un incident de sécurité va se produire, mais « quand ». Une PME/PMI doit, elle-aussi, s'y préparer selon sa taille, et surtout selon les conclusions de son analyse de risques.

Principe n° 9 : Mettre en place un plan solide de reprise après sinistre en cas de cyberattaques

La société dépend de plus en plus de la technologie et les cyberattaques se multiplient, il est donc essentiel que toutes les organisations, quelle que soit leur taille, se préparent au pire. Les stratégies de reprise de la sécurité doivent être réexaminées et mises à jour fréquemment.

Principe n° 10 : Instaurer une culture de la cybersécurité

L'évolution de l'environnement de l'entreprise implique que son périmètre de sécurité s'est déplacé vers les utilisateurs et leurs multiples terminaux. L'identité est devenue le nouveau périmètre, tout utilisateur au sein de l'entreprise se retrouve ainsi en charge d'une certaine part de responsabilité en matière de cybersécurité.

En partant du Principe n° 1 qui recommande d'"Adopter la mentalité d'un dirigeant d'entreprise" on en arrive au Principe n° 10 qui suggère d'"Instaurer une culture de la cybersécurité". Encore une fois, il s'agit bien d'intégrer la cybersécurité dans l'ADN de l'entreprise.

Intégrer la cybersécurité dans l'ADN de l'entreprise

Le point de départ est donc que le dirigeant de l'entreprise prenne la mesure de sa responsabilité. De nos jours, l'infrastructure informatique est complexe, distribuée, basée sur le cloud, avec une adoption rapide (maîtrisée ou imposée) de l'intelligence artificielle. Dans ce contexte, il devient impératif que le dirigeant comprenne, quand bien même le discours du Responsable de la Sécurité des Systèmes d'Information n'est pas assez explicite, que les enjeux sont en termes de réduction des risques, de prévention des pertes, de continuité des activités, de protection de la valeur actionnariale. Une fois cette prise de conscience réalisée, le dirigeant adopte une approche structurée, qui commence par la gouvernance de la cybersécurité, qui intègre la formation et la sensibilisation de tout le personnel, qui prend appui sur des solutions technologiques intelligentes. Cette approche structurée se traduit par un ensemble d'attitudes et de comportements auxquels adhère le dirigeant d'entreprise. Ses capacités de leadership en sont plus renforcées par exemplarité et implication active.

La norme ISO 27001 est un cadre organisationnel et processuel qui apporte de nombreuses solutions dans cette approche structurée. Des éléments d'attitudes et de comportements sont proposés ci-dessous pour composante de cette approche. De manière plus précise, chacun des 10 Principes trouve son axe d'application dans cette norme ISO 27001. Les articles qui suivront en offriront les détails, avec l'ambition de fournir le maximum d'orientations pour l'acceptation, l'assimilation et la mise en application de ces principes.

La référence à la norme ISO 27001 peut prêter à sourire si l'on considère que cela revient à « utiliser un marteau pour tuer une mouche ». Mais ce n'est évidemment pas le cas. Quel que soit l'outil utilisé pour tuer la mouche, il requiert de l'énergie, de la rapidité et de la précision. En cela, la norme ISO 27001 est très attachée au principe fondamental de proportionnalité. Les actions doivent être justifiées par une analyse des risques objective afin d'éviter des coûts ou des freins opérationnels inutiles. La certification n'est pas une obligation; il convient d'abord de raisonner en termes d'avantages opérationnels, d'atouts commerciaux et de gains de productivité grâce à l'amélioration continue des

Intégrer la cybersécurité dans l'ADN de l'entreprise signifie que le dirigeant d'entreprise a imprégné la cybersécurité dans la raison d'être de l'entreprise, sa vision et ses valeurs. Cet ensemble d'attitudes et de comportements est assez important pour mériter l'attention du Forum Économique de Davos. En tant que dirigeant et chef d'entreprise, si vous ne pensez pas cybersécurité pour protéger vos actifs et pour ajouter de la valeur à vos produits et services, vous devez au minimum chercher à éviter que votre entreprise soit la porte par laquelle le mal s'introduit chez vos clients, partenaires, prestataires.