Chapitre 5
Technologies de protection de données

1. Introduction

1.1 Un peu d'histoire

Il y a une vingtaine d'années, le titre de ce chapitre et même de cet ouvrage aurait probablement été simplement « Meilleures pratiques en matière de sauvegarde des données ». Un tel titre n'a plus de sens aujourd'hui en raison des évolutions successives des technologies de protection de données au fil des différentes ères informatiques.

La nécessité de conserver une copie des données s'est rapidement fait sentir dès l'avènement des premiers ordinateurs. Avant l'an 2000 qui marque le début de la bulle financière d'Internet et des premières start-up, aucune solution de sauvegarde à proprement parler et digne de ce nom existe alors.

La protection de la donnée ou de tout fichier se limite à copier celui-ci sur un autre support de stockage, par exemple la disquette informatique initialement utilisée. Une fois la copie des fichiers terminée, on l'extrayait de l'ordinateur, on la rangeait alors dans une boîte prévue à cet effet, pourvue d'une petite clé, disposée sur le bureau ou au mieux dans l'armoire adjacente.

Les risques afférents à la cybercriminalité n'étaient à l'époque pas d'actualité. L'administrateur ou l'opérateur en question devait se charger d'identifier manuellement au stylo le support de stockage et surtout se souvenir du lieu de stockage de la copie. Les informations portées sur le support se limitaient au strict minimum. Néanmoins, les indications manuscrites devaient être suffisamment précises pour retrouver rapidement la copie de la donnée au besoin. Les systèmes étaient fortement centralisés et chaque ordinateur disposait de son propre disque dur et de son propre lecteur de disquettes ou au mieux lecteur de bande magnétique.

L'avènement du réseau informatique permet par la suite d'interconnecter les ordinateurs entre eux. Il simplifie le transfert des données sans pour autant changer réellement la problématique de sauvegarde des données. Les copies sont orchestrées de manière quotidienne. La sauvegarde manuelle ou non se fait au mieux en fin de journée, sinon quand on y pense.

1.2 Une période sombre pour les données

Cette période de l'Âge sombre du numérique est néanmoins marquée par la perte de bon nombre de données, faute de les avoir sauvegardées dans les règles de l'art. On peut notamment citer le manque de viabilité et de fiabilité des premiers supports informatiques, très vulnérables à l'environnement extérieur (variation de températures, choc physique, champ électromagnétique…), l'absence de normes ou de standards au niveau des systèmes informatiques, l'utilisation de formats de données propriétaires ou devenus obsolètes...

Les conséquences de ces pratiques sont parfois catastrophiques. En 1975, la NASA lance le programme Viking, dont l'objectif est de faire atterrir sur Mars les premiers engins spatiaux américains. Au terme de la mission, il faudra quelque dix années avant de pouvoir procéder à l'analyse des bandes magnétiques contenant les enregistrements de la phase d'atterrissage des engins sur le sol martien.

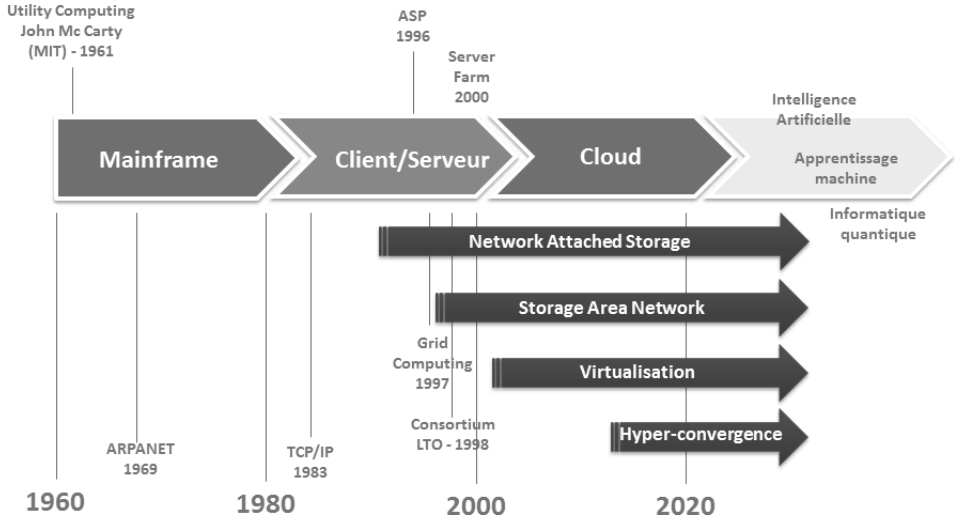
Un problème de taille se pose alors aux scientifiques de l'époque quant au bon déroulement de cette analyse. Le format de données était entièrement propriétaire et totalement inconnu des analystes de l'époque. Pire encore, les développeurs à l'origine du système d'enregistrement étaient décédés dans l'intervalle ou avaient quitté la NASA. Il n'existe alors aucune documentation technique sur le format employé.

Plusieurs mois d'analyse et d'ingénierie inverse (*reverse engineering*) seront nécessaires à l'extraction des précieuses données de ce qu'il convient d'appeler une véritable boîte noire. Si une telle situation n'est plus souhaitable à l'heure actuelle, il convient de garder à l'esprit l'aspect pérennité des données sauvegardées, mais également le facteur humain, car les acteurs d'aujourd'hui ne seront pas forcément ceux qui procéderont à la restauration demain.

1.3 Voguent les données

Les évolutions technologiques successives en matière d'informatique ont des répercussions directes sur le volume de données produit et échangé quotidiennement au niveau mondial. Elles influent également sur la manière dont tout un chacun y a accès et enfin sur les moyens à mettre en œuvre pour en garantir la disponibilité et la résilience.

Au début du XXI^{e} siècle, la donnée devient le sujet de toutes les convoitises et quelques entreprises américaines comprennent rapidement l'importance de la collecter à grande échelle afin de la monétiser, et ce, très souvent à l'insu de son propriétaire. La donnée est désormais « l'or Invisible » de ce siècle et les GAFAM (Google Amazon Facebook Apple Microsoft) l'ont parfaitement saisi. Les technologies de protection de données actuelles sont nées des concepts majeurs ayant traversés les différentes ères informatiques.



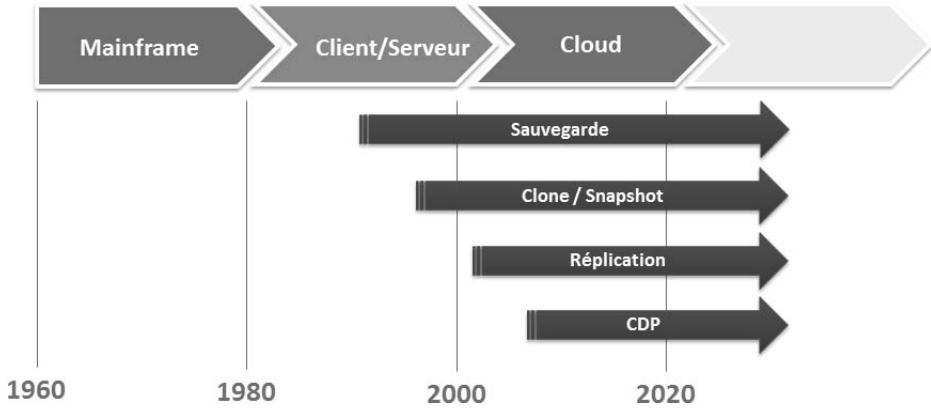
1.4 Des nouvelles exigences et nouvelles technologies

Le 1er janvier 1983, le réseau ARPANET adopte le protocole TCP/IP, la base d'Internet. La volatilité des supports de stockage, associée à une plus grande mobilité des données susceptibles désormais d'être échangées, et au temps de traitement nécessaire pour obtenir un résultat issu d'un calcul, se double de l'impératif de préserver les informations.

Les premières solutions de sauvegarde mettant en application trois principes majeurs apparaissent vers la fin des années 1980. Les autres technologies de protection de données, à savoir la réplication, le cliché instantané (*snapshot*) puis la protection continue des données (CDP - *Continuous Data Protection*) viennent épauler les solutions de sauvegarde traditionnelles ; ces dernières ne suffisant pas toujours à répondre favorablement aux nouvelles exigences en matière de résilience et de disponibilité des données.

Remarque

La protection des données n'est pas une simple affaire de sauvegarde et de restauration, mais un ensemble de processus, méthodes et technologies à mettre en œuvre, constituant une fonction régalienne de toute entreprise publique ou privée.

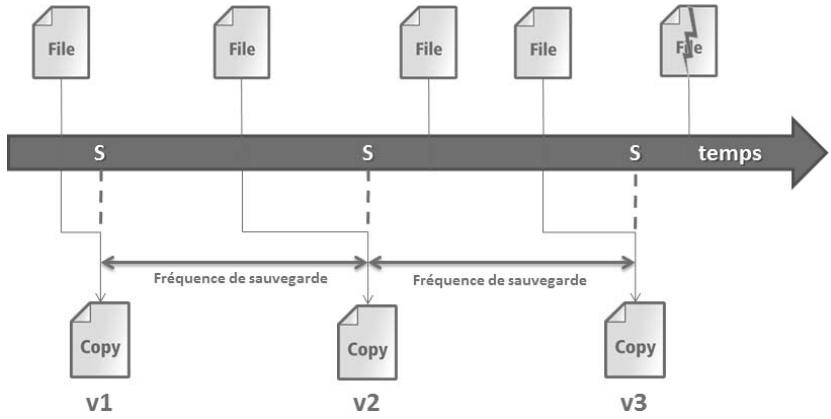


1.5 Les familles SPit et APiT

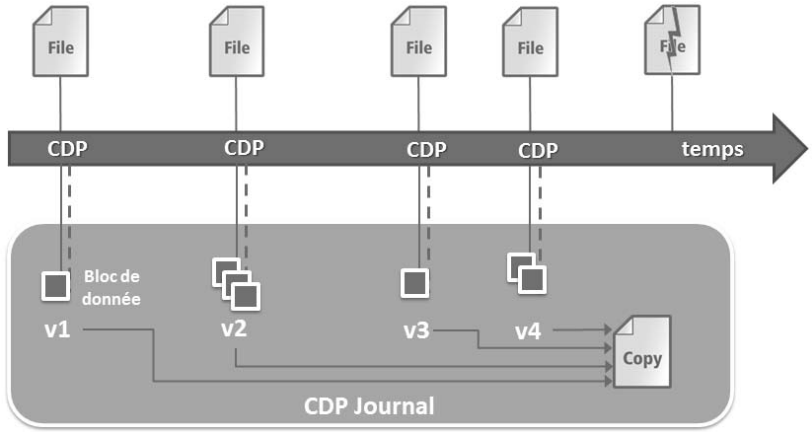
Les technologies de protection des données énoncées précédemment peuvent être classées en deux grandes familles distinctes.

1.5.1 APiT (Any Point-in-Time)

Il convient de traduire l'acronyme APiT (*Any Point-in-Time*) par « à tout instant dans le temps », en l'occurrence dans le passé. Les solutions de sauvegarde traditionnelles appartiennent naturellement à cette famille. Le principe de mémorisation décrit plus loin dans ce chapitre à la section Les trois principes élémentaires est mis à contribution par la sauvegarde afin de pouvoir restaurer une donnée à un instant précis dans le temps. Toute technologie appartenant à cette famille est par conséquent à même de conserver plusieurs versions d'une même donnée et de les restaurer, à la demande, depuis un historique plus ou moins important selon la technologie utilisée et la durée de conservation paramétrée.



Il convient de pondérer le terme « à tout instant dans le temps ». La restauration d'un fichier traditionnel se matérialise par une version disponible parmi celles mémorisées lors des différentes sauvegardes. En revanche, la réalisation de sauvegarde « à chaud » de bases de données relationnelles permet de restaurer celles-ci à un instant très précis, tel qu'une transaction, en exploitant les mécanismes de journalisation. L'exemple ci-dessus illustre, ici, la restauration de trois versions de sauvegarde d'un même fichier alors que celui-ci a fait l'objet de quatre modifications. La fréquence de sauvegarde détaillée ultérieurement est ici supérieure à celle de la modification du fichier. Fort de ce constat, la technologie de protection continue des données (*Continuous Data Protection* - CDP), appartenant à cette même famille, résout ce problème.



Grâce à cette technologie, tout bloc de données modifié au niveau d'un fichier par exemple est immédiatement enregistré comme une nouvelle version du fichier dans un fichier de journalisation : le CDP Journal. Le temps séparant l'écriture de la donnée sur le stockage primaire et l'enregistrement du ou des blocs modifiés dans le journal CDP va être déterminant pour définir si la technologie est dite « *Near CDP* » ou « *True CDP* ». Certaines solutions de protection de données mettent en œuvre la technologie CDP au moyen d'un ordonnanceur. Celui-ci déclenche à un intervalle de temps très rapproché (tous les quarts d'heure ou moins, par exemple) un cliché instantané afin de procéder à l'écriture du ou des blocs de données modifiés dans le journal CDP. La technologie est alors « *Near CDP* ». Dans le cas contraire, ces deux opérations sont quasi synchrones.

1.5.2 SPiT (Single Point-in-Time)

Il convient de traduire cet acronyme dans la langue de Molière par « un seul instant dans le temps ». En d'autres termes et contrairement aux technologies appartenant la famille APiT, une seule version de la donnée est conservée. Cette dernière version est la plus à jour possible. On parle alors de « fraîcheur » de la donnée. La réplication des données appartient à cette famille. Cette technologie de protection des données est largement répandue afin de disposer des données les plus à jour sur un site de secours. La technologie de réplication est mise en œuvre à différents niveaux de l'infrastructure, qu'il s'agisse de répliquer des fichiers, des fichiers journaux d'une base de données, des machines virtuelles, des volumes disques (LUN) entiers ou encore une copie de données précédemment sauvegardée sur disque. La réplication s'exécute selon des modes synchrone ou asynchrone détaillés ultérieurement.

Chapitre 3
La norme ISO 27001

1. Contextualisation de la norme

La norme ISO 27001 est, à l'instar des standards ISO 9001 (qualité) et ISO 14001 (environnement), une norme de gouvernance. La gouvernance étant définie comme le processus qui consiste à contrôler l'utilisation des actifs et ressources pour accomplir la mission de l'organisation. La norme ISO 27001 est dévolue à la sécurité de l'information, et a donc pour objectif d'améliorer la gestion des actifs et des ressources en termes de cybersécurité. Il convient de prendre en considération au premier chef cette essence managériale, et comprendre de prime abord que, loin d'être réservée aux seuls spécialistes de la cybersécurité, elle est destinée plus largement à un public ayant à mettre en place et opérer un système de gouvernance. Dans bien des organisations, des responsables qualité au fait de l'ISO 9001 ont mis en place avec succès une gouvernance sécurité, quand l'appropriation de la norme par des spécialistes techniques de la sécurité s'est avérée plus délicate. Et c'est bien naturel, puisque toutes ces normes de gouvernance présentent un modèle similaire, et spécifient les mêmes règles.

La norme ISO 27001 n'est donc pas réservée à une minorité d'élus spécialistes de la technologie ; elle n'est pas non plus exclusivement réservée à de grands groupes, et bien des PME ont été certifiées ces dernières années, ou ont mis en place avec succès ce modèle de gouvernance. Nous reviendrons sur le côté flexible du standard, sur les possibilités d'amélioration continue qu'il offre et qui le rend adaptable aux budgets plus restreints de structures moins bien dotées.

La norme ISO 27001 fait partie d'un ensemble normatif regroupé sous le sigle ISO 2700X. C'est la seule norme de cet ensemble qui donne lieu à certification, c'est-à-dire que des organismes accrédités peuvent certifier la conformité d'un organisme au standard.

La norme 27001 s'inscrit dans un corpus documentaire plus global, qui comprend essentiellement les éléments suivants :

– ISO 27002 : code de bonnes pratiques pour le management de la sécurité de l'information; il constitue une liste de mesures qu'il est recommandé de prendre en compte pour réduire les risques ou améliorer son niveau de sécurité. Ces mesures constituent l'annexe A de la norme ISO 27001.
– ISO 27003 : guide pour mettre en place la norme ISO 27001.
– ISO 27004 : guide pour la définition d'indicateurs visant à contrôler la pertinence et l'efficacité des mesures mises en place.
– ISO 27005 : guide relatif à la gestion des risques.

2. Rappel historique sur sa construction

Sans être un amateur inconditionnel du duc de Bern, il est des cas où un peu d'histoire permet de donner un éclairage neuf à une situation présente ; et c'est effectivement le cas pour la norme ISO 27001.

La norme ISO 27001 est en fait de naissance britannique, et existait avant son adoption à l'ISO au tournant du siècle en tant que standard BS (*British Standard Organisation*) sous la référence 7799-1 (7799-2 pour ce qui devait devenir ISO 27002). Est-ce cette naissance britannique qui a conduit les Français à adopter une position très réservée à l'égard de ce qui devait devenir le seul standard de sécurité réellement utilisé par le monde ? Peut-être est-ce effectivement lié à une inimitié remontant à Jeanne d'Arc… Peut-être et plus vraisemblablement est-ce lié au côté, non pas libertaire, mais respectueux de la liberté d'entreprendre que peuvent parfois avoir nos voisins d'Outre-Manche et qui nous fait souvent défaut ? Peut-être ce standard est-il beaucoup trop pragmatiquement anglais et heurte le goût français du dogmatisme ?

Le standard est respectueux de la liberté d'entreprendre. Dans la mesure où le système de management est en phase avec les objectifs stratégiques fixés par la direction, où il est conforme aux exigences réglementaires et au cadre contractuel que l'entreprise s'est fixé, il est possible d'agir en toute liberté. On est effectivement loin d'une école de pensée française friande de règles, qui génèrent autant d'exceptions, règles que nous subissons depuis l'école primaire.

Le standard est pragmatique, il définit la démarche à suivre et ne contraint pas le chemin. Il n'impose pas non plus le périmètre à traiter. Une analyse de risques doit être effectuée, le standard ne définit pas de méthode, juste une démarche. Une fois les risques identifiés, l'entreprise est libre de ses choix de traitement dans la mesure où les objectifs, la réglementation et les exigences contractuelles sont respectés. On est loin du dogme, il n'existe pas de vérité absolue, juste des objectifs à atteindre, des risques qui limitent l'atteinte de ces objectifs, et des mesures que l'on peut mettre en place ou non, en fonction de ses moyens, de sa maturité, dans la mesure où l'on tend vers une situation maîtrisée dans un futur raisonnable.

Du pragmatisme, peu de règles, et peu d'enthousiasme de la France, qui connaît un retard assez important dans l'adoption du standard par ses entreprises. Retard qui tend petit à petit à se résorber, mais reste très important au regard des Japonais férus de normes, ou de nations anglophones ayant compris très rapidement les avantages économiques d'une certification.

3. Domaine adressé

La norme 27001 est donc avant tout une norme de gouvernance, appliquée à la sécurité de l'information. Elle permet de définir un Système de Management de la Sécurité de l'Information (SMSI). Il convient alors de définir le sens donné à « sécurité de l'information » : la sécurité de l'information est un processus visant à protéger des données contre l'accès, l'utilisation, la diffusion, la destruction, la modification non autorisée ou l'indisponibilité. Le point important à retenir dans cette définition, en dehors de l'introduction des concepts de confidentialité d'intégrité et de disponibilité qui seront développés ultérieurement, est la composante protection des données : le système de management vise à protéger les données qui le nécessitent, quel que soit leur support (papier, clé USB, espace mémoire, bande de sauvegarde…), qu'elles soient échangées ou stockées… Il convient également de noter qu'il n'y a pas de restriction envisagée quant à la notion de protection : le système de management fera ainsi appel à des mesures physiques (accès aux locaux, caméra…), techniques (sécurité des postes de travail, sécurité des réseaux, des systèmes…), des mesures organisationnelles (recrutement, sensibilisation…) ou des mesures procédurales (définition de politiques, de procédures…).

Cela signifie implicitement, mais il est bon de le souligner, que la mise en place du système de management de la sécurité de l'information va bien au-delà des seules directions informatiques et implique également la direction logistique, la direction des ressources humaines, la direction juridique, etc.

La norme adresse donc la gouvernance de la sécurité de l'information. Mais à qui est-elle destinée ? Si l'on se reporte à la définition première, à toute entreprise concernée par la protection de ses données contre l'accès, l'utilisation, la diffusion, la destruction, la modification non autorisée ou l'indisponibilité. Ce qui concerne, somme toute, l'ensemble des entreprises de la planète. Quelle entreprise pourrait ne pas se soucier d'une perte de son fichier client, d'une indisponibilité de son système de production, d'une modification des données de facturation ou de paie ? Ou de maltraiter les données personnelles qui lui sont confiées ? Il convient de raison garder et d'adopter un peu de pragmatisme. Chaque entreprise devrait se poser les questions suivantes : est-ce que je traite des données sensibles ? Est-ce que ces données sont sensibles au point que leur perte, leur altération, leur indisponibilité auraient un impact conséquent sur ma structure ? Et cet impact est-il conséquent au point que le coût de ma gouvernance sécurité est justifié ? La logique est un peu la même que pour la sécurisation de son appartement. Vais-je investir dans un système d'alarme très sophistiqué si je n'ai pour toute richesse qu'un grille-pain et une télévision ? La réponse est non, évidemment. Sauf si l'on tient résolument à son grille-pain.

À cela s'ajoute le constat suivant, qui a toute son importance : la norme laisse à l'entreprise le choix de son domaine d'application, c'est-à-dire du périmètre sur lequel porte le système de management. En d'autres termes, il est possible, et même tout à fait souhaitable, de circonscrire la portée du système de management aux seuls processus comportant des données vraiment stratégiques pour l'entreprise : l'offre SaaS pour un éditeur logiciel, l'hébergement pour un datacenter, l'activité d'audit pour une société de service… Pour reprendre le parallèle avec la sécurisation de l'appartement, la norme vous invite à choisir la pièce à sécuriser, parce que c'est celle où vous exposez vos tableaux, celle où vous recevez vos invités, votre cave si vous êtes porté sur la bouteille, non, si vous êtes un œnologue averti. L'investissement peut donc être contrôlé et progressif, au sens où il est possible de commencer par un périmètre limité, et de l'étendre par la suite.

L'adoption de la norme peut avoir également d'autres causes que la seule amélioration de la maturité sécurité : obligations contractuelles, avantages concurrentiels, accès à de nouveaux marchés… qui sont abordés dans la prochaine section.

4. Usage actuel de la norme

Dans ses grandes lignes, la norme ISO 27001 incite une organisation à définir un plan d'action afin de se mettre en conformité vis-à-vis des exigences réglementaires et de ses engagements contractuels, et d'atteindre les objectifs de sécurité qu'elle s'est fixée en réduisant les risques par la mise en place de mesures. Elle demande également de contrôler l'efficacité de ces mesures au travers d'indicateurs. Elle demande enfin et surtout de mettre en place ce plan d'action, et d'améliorer les éléments qui demeurent perfectibles au regard des audits, des indicateurs et plus généralement des opportunités constatées. Il s'en suit que la norme invite à améliorer progressivement sa maturité sécurité, en harmonie avec les moyens humains et financiers de l'entreprise. Elle est en cela pragmatique : on constate en effet trop d'organisations qui, confrontées à un référentiel sécurité trop contraignant, abandonnent tout simplement l'exercice ; un peu comme on ne retourne pas dans un club de sport qui vous propose un entraînement inadapté à vos capacités du moment. La norme a cette vertu de se montrer accessible à tous, et de permettre un développement harmonieux et progressif de la maturité sécurité.

Deuxième atout conséquent de la norme : sa cohérence avec les autres standards de gouvernance que sont l'ISO 27001 et l'ISO 14001, et plus généralement les pratiques de management de toute entreprise. Cette cohérence ancre la communication avec le Directeur Informatique ou le Directeur Général en terrain connu. Quel RSSI (responsable de la sécurité du système d'information) n'a pas connu de grands moments de solitude en présentant un budget non argumenté, et pour tout dire peu compréhensible, à sa direction ? Comment justifier une ligne de 30000 euros d'équipements de sécurisation réseau, une autre à 20000 euros pour la sécurisation des postes de travail… ?

La norme permet de placer la relation dans une situation familière à la direction, et ce faisant rend la discussion plus aisée : la direction a fixé des objectifs stratégiques, le RSSI a décliné ces objectifs stratégiques en objectifs de sécurité ; il a analysé les exigences réglementaires, contractuelles, mesuré les risques de ne pas atteindre ses objectifs et propose des mesures, des coûts, un planning, afin d'atteindre lesdits objectifs. Il a priorisé ces mesures et a défini des éléments de contrôle de l'efficacité de celles-ci. Il peut donc en justifier les coûts : telle mesure coûte tant, permet d'atteindre 40 % de mon objectif, sera en place dans huit mois, et nous serons ainsi en phase avec tel engagement contractuel. Il peut également, au travers des indicateurs, reporter à sa direction de l'avancement du chantier correspondant, et montrer l'efficacité de la mesure planifiée au travers d'indicateurs soigneusement choisis. La direction, en retour, peut suivre l'intérêt de son investissement et la cohérence des dépenses effectuées.

4.1 Obtenir la certification ISO 27001

Au-delà de l'amélioration de la maturité sécurité, l'objectif fixé par la direction peut être d'obtenir la certification ISO 27001 sur un périmètre donné. Les motivations incitant une entreprise à aller jusqu'à la certification sont développées dans les paragraphes suivants. Tentons dans un premier temps d'effectuer un point sur le nombre de certifications, même si cela n'est pas chose aisée.

La France atteint en 2018 la vingt-quatrième place mondiale, avec un nombre d'entreprises certifiées peu ou prou au niveau de la Belgique. Le Japon occupe la pôle position mondiale, les pays européens étant somme toute bien représentés puisque l'Allemagne et l'Italie sont dans le top 6.

Notons qu'en 2019, 60 000 sites sont certifiés dans le monde, chiffre à rapprocher de 1 200 000 sites certifiés ISO 9001. On voit que l'écart est encore conséquent quant à l'appropriation des standards par les entreprises. Cependant, les mêmes sources notent une progression sur l'année de 19 % dans le monde, et font même état de 63 % en France.