Il y a trois types d'effacement connus. Le premier est la suppression du fichier en le mettant dans la corbeille et on la vide par la suite. Ce type d'effacement ne supprime que la première lettre du fichier et une petite partie dans les métadonnées. Les données restent donc accessibles en utilisant un outil qui permet de traiter de l'hexadécimal. Le deuxième type d'effacement est le formatage de disque dur. Cela supprime la première table de partition en effaçant qu'une partie des références. Les données pourront toujours être récupérées. Le troisième mode d'effacement consiste à faire un FDISK c'est à dire un re partitionnement. Ce dernier non plus n'est pas totalement efficace. La seule solution pour effacer des données est d'utiliser un logiciel qui écrase les données par une réécriture et donc de faire un WIPE du disque. « Les solutions qu'on a trouvé sur le marché et qu'on a analyser en tant que spécialiste de récupération de données, montre que ces solutions sont inégales et que souvent plus de 50% des données sont encore exploitables malgré un WIPE du disque »

L'être Humain reste au cœur de la sécurité des systèmes d'information

85% de la menace vient de l'être Humain dans une entreprise. Il ne suffit pas donc de se doter des logiciels et des outils de sécurisation de données, de cyberdéfense et de garantie de continuité de l'activité, mais il faut aussi sensibiliser les collaborateurs et cela à tous les niveaux autour de la sécurité de l'information.

Cet avis est partagé par Frédéric Descamps, le responsable marché de la société française aDvens. « En sensibilisant, en formant, en apportant de l'information, on contribue grandement à améliorer le niveau général de sécurité dans une entreprise, notamment en agissant sur l'être Humain qui doit passer du maillon faible de la sécurité vers le maillon fort ». Il a aussi précisé « La sécurité, on en fait pas pour en faire, la sécurité doit être au services des enjeux business des clients ».

Il faut tout d'abord définir son référentiel sécurité en se basant sur les normes et les réglementations. La norme ISO 27001 pose le cadre du Management de la Sécurité de l'Information au sein d'une entreprise. Elle encourage l'adoption d'une démarche de gestion orientée processus et s'appuie sur le modèle PDCA (Plan Do Check Act) -voir figure 1-

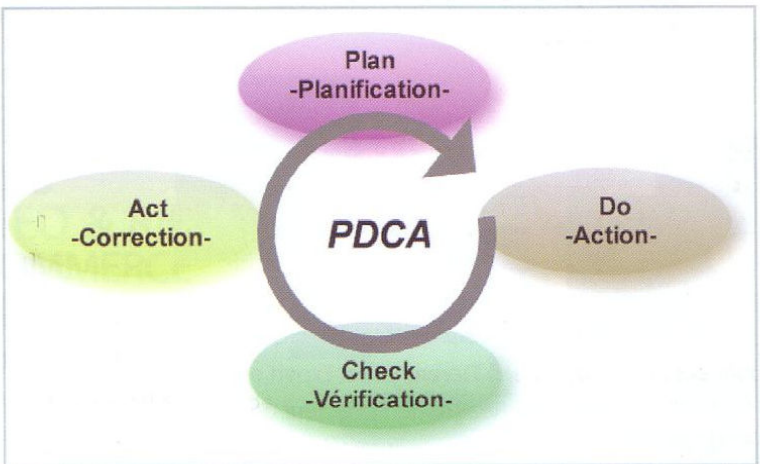

Figure 1 : PDCA>>

Quant à la clé USB qui est souvent utilisé comme moyen pour piéger des entreprises et ouvrir des failles afin d'attaquer le système, Frédéric Descamps propose de mettre un ordinateur de test à l'entrée des bureaux afin de vérifier l'intégrité et la sécurité des clés USB. En effet interdire purement et simplement les clés USB dans une entreprise peut nuire à la productivité. En ce moment il y a une forte propagation du ver « Conflicer » qui est notamment dû à des clés USB infectées. Il devient nécessaire de sensibiliser sur la dangerosité potentiels des clés USB. Le collaborateur doit devenir acteur de la sécurité de l'information.