Octobre 2013

Centre Africain d'Etudes Supérieures en Gestion

CESAG BF – CCA
BANQUE, FINANCE, COMPTABILITE, CONTROLE & AUDIT

MPCGF 1 - MPTCF

Promotion 9
(2010-2011)

Mémoire de fin de formation
pour l'obtention de la Maîtrise Professionnelle de Techniques Comptables et Financières (MPTCF)

THEME

ASSURANCE QUALITE D'UNE POLITIQUE DE SECURITE INFORMATIQUE :

« CAS DE LA SOCIETE ENERGETIQUE STAR OIL »

Présenté par :

Soda Marieme FALL

Dirigé par :

Mouhamed El Hafed DIALLO
Manager du Cabinet Eureka Audit & Conseils

Octobre 2013

DEDICACE

Nous dédions ce mémoire à notre mère Maimouna Sy et à notre père Abdou Fall, pour les sacrifices consentis, la patience et les encouragements à notre endroit, mes frères et moi. Qu'ils trouvent dans ce modeste travail l'aboutissement de leurs nombreux efforts.

REMERCIEMENTS

Nous tenons à remercier :

- ✓ nos parents Maimouna Sy notre maman et Abdou Fall notre père qui nous couvent et nous portent vers le succès ;
- ✓ nos frères et sœurs ;
- ✓ nos grands parents ;
- ✓ nos cousins et cousines ;
- ✓ nos oncles et tantes ;
- ✓ nos amis ;
- ✓ nos camarades de promotion ;
- ✓ le CESAG pour la qualité de l'encadrement et de la formation reçus ;
- ✓ M. Babacar Wade qui aura suscité en moi la passion pour ce métier ;
- ✓ M. Mouhamed El Hafed, qui m'a encadré pour la réalisation de ce mémoire ;
- ✓ M. Assane Kane, pour son inestimable contribution ;
- ✓ l'ensemble du personnel du cabinet Eureka Audit & Conseil ;
- ✓ l'ensemble du personnel de Star Oil ;
- ✓ tous ceux, qui de près ou de loin, ont contribué à la réalisation de ce mémoire.

LISTE DES SIGLES ET ABREVIATIONS

DSI : Directeurs des Systèmes d'Information

FTLS Formal Top Level Specification

IFRS: International Financial Reporting Standards

ISO : International Organization for Standardization

NTIC : Nouvelles Technologies de l'Information et de la Communication

OIN : Organisation Internationale de Normalisation

RSI : Responsable du Système Informatique

RSSI : Responsable de la Sécurité du Système d'Information

SI : Système d'Information

SWIFT : Social for Worldwide Interbank Financial Télécommunications

TCB : Trusted Computing Base

TIC : Technologie de l'Iinformation et de la Communication

LISTE DES TABLEAUX ET FIGURES

➢ TABLEAUX

➢ FIGURES

TABLE DES MATIERES

INTRODUCTION GENERALE

Aujourd'hui, les nouvelles technologies de l'information et de la communication (NTIC) ont une importance capitale dans le monde. En ce début de troisième millénaire, les NTIC ont réduit notre planète à l'échelle d'un « village global » selon l'expression de Marshall McLuhan.

Le progrès remarquable des technologies de l'information et de la communication au cours des dix dernières années a fait naître un grand nombre de systèmes d'information dans les organisations et administrations. Ces systèmes d'information, moteurs de croissance et de développement des métiers et services sont assez importants, voire même indispensables pour le bon fonctionnement de toute entreprise. Cependant, avec les menaces actuelles et les ouvertures des systèmes d'information sur l'internet et d'autres réseaux non maîtrisés, il devient nécessaire de garantir la sécurité de l'ensemble des biens constituant tout système d'information.

L'assurance qualité de la sécurité du système informatique est devenue ainsi plus qu'une nécessité, l'importance de posséder un système informatique fiable est vital pour une entreprise. L'assurance qualité est définie dans l'ISO 8402 comme « l'ensemble des activités préétablies et systématiques mises en œuvre dans le cadre du système qualité et démontrées en tant que besoin pour donner la confiance appropriée en ce qu'une entité satisfera aux exigences pour la qualité.» Les statistiques des attaques et des menaces font que les responsables sont conscients aujourd'hui des risques pesant sur un système d'information et mettent tous les moyens en œuvres afin d'assurer effectivement et efficacement la sécurité. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et contrôler le système informatique.

L'informatique accompagne désormais toute les activités de l'entreprise. Il est donc indispensable, non seulement de se préoccuper de la performance du système informatique en place, mais aussi de veiller à sa sécurité permanente. La sécurité du système d'information d'une manière générale dans une entreprise, est un requis important pour la poursuite de ses activités. Qu'il s'agisse de la dégradation de son image de marque, du vol de ses secrets de fabrication ou de la perte de ses données clients ; une catastrophe informatique a toujours des conséquences fâcheuses pouvant aller jusqu'au dépôt de bilan.

On doit réfléchir à la mise en place d'une politique de sécurité informatique avant même la création du réseau. Le système informatique représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique rassemble donc les problématiques qui visent à empêcher que par son canal, l'on puisse nuire à l'entreprise, en l'espionnant ou en la décrédibilisant. Une politique de sécurité informatique est donc l'ensemble des moyens mis en

œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

C'est dans cette optique que les entreprises américaines depuis quelques années, face à la recrudescence de la cybercriminalité, du piratage de leur système informatique, se sont vues obliger de renforcer leur système de sécurité informatique. En France, par ailleurs le même phénomène s'observe notamment au travers les pirates informatiques.

Ceci est d'autant plus valable pour nos états africains qui à l'instar de leurs semblables des autres continents, veulent assurer la qualité de leur système informatique.

Les entreprises sénégalaises suivent le rythme évolutif dans ce monde marqué par une avancée fulgurante des connaissances en technologie de l'information et de la communication (TIC).

En effet, dans leur majorité l'assurance qualité du système informatique est devenue essentielle à leur croissance, en particulier pour les entreprises énergétiques sénégalaises. Cette situation justifie que ces dernières prennent une série de mesures selon leurs besoins de sécurité et les moyens à disposition. Les possibilités dans ce domaine vont de l'adoption de mesures techniques ou organisationnelles à la protection de l'ensemble du système.

L'organisation étudiée notamment la Star Oil qui est une entreprise énergétique dispose d'un management qui a le souci de sécuriser son système d'information et a mis en place depuis quelques années des moyens afin de sécuriser son système informatique.

L'inexistence du point de vue administratif d'un manuel de procédure de gestion du système informatique ainsi que la timide implication des responsables de la société, accordent peu de place à la qualité d'une politique de sécurité informatique. Cet état de fait augmente la probabilité qu'un risque majeur puisse se matérialiser et menacer l'intégrité du système.

Notons que la défaillance de la qualité d'une sécurité informatique peut être causée par :

- ✓ l'absence d'un département de l'audit informatique ;
- ✓ l'absence de Risq manager ;
- ✓ le manque d'effectifs nécessaires ;
- ✓ l'absence de mise en place de mesures adéquates d'une sécurisation de l'informatique ;
- ✓ la méconnaissance des nouvelles menaces sur le système ;

- ✓ la non-connaissance par l'utilisateur des fonctionnalités du système pouvant lui être nuisibles ;
- ✓ la méconnaissance des moyens de sécurité mis en place…

Les conséquences découlant du problème mentionné ci-dessus peuvent être :

- ✓ l'indisponibilité d'une sécurité informatique dans l'entreprise ;
- ✓ les pertes de donnée ;
- ✓ les vols de donnée ;
- ✓ le piratage du système informatique ;
- ✓ divulgations de données confidentielles de l'entreprise…

Afin d'y faire face les mesures suivantes peuvent être envisagées :

- ✓ mettre en place d'un département de l'audit informatique ;
- ✓ nommer un Risq manager ;
- ✓ diagnostiquer la politique du système informatique ;
- ✓ s'assurer de la qualité du système informatique mise en place…

La dernière solution parait la plus opportune car l'assurance qualité du système informatique permettrait de déceler les anomalies et insuffisances du système en vue d'une meilleure gestion depuis la conception, passant par l'analyse jusqu'à la mise en place.

Au regard de ce qui précède la question principale à laquelle ce mémoire répondrait est la suivante : comment la sécurité du système informatique est t'elle assurée ?

Elle conduit aux questions spécifiques suivantes :

- ✓ Quel est l'importance de l'assurance qualité du système informatique ?
- ✓ Quel est le rôle de la direction dans l'assurance qualité du système informatique ?
- ✓ Comment identifier les risques liés à défaillance du système informatique ?
- ✓ Comment élaborer une politique de sécurité informatique efficace ?

L'étude de l'assurance qualité de la politique de sécurité informatique de la Star Oil permettra de répondre à ces questions à travers les objectifs spécifiques suivants :

- ✓ définir ce que c'est qu'une politique de sécurité informatique ;
- ✓ donner l'importance de l'assurance qualité de la politique de sécurité informatique ;
- ✓ énoncer les raisons de recourir à l'assurance qualité de la sécurité informatique ;
- ✓ établir la démarche d'élaboration de l'assurance qualité de la sécurité informatique.

L'objectif principal de notre étude se limitera à s'assurer de la qualité du système informatique de la Star Oil et à faire des propositions en cas de faiblesses identifiés.

L'intérêt de cette étude pour l'entreprise Star Oil est de pouvoir cerner les risques liés à son système informatique à travers les faiblesses identifiées. Cela, afin de faire des propositions allant dans le sens de l'amélioration de celui-ci. Ce qui devra contribuer à une prise de conscience du présent et à une vision de l'avenir de la part des responsables.

Ce sujet suscite de notre part un véritable intérêt, dans la mesure où son étude permettra de mieux connaître cet élément stratégique qu'est l'assurance qualité d'une sécurité informatique et d'appréhender son impact sur les entreprises. Mais aussi, de proposer un document qui permettra de comprendre et de saisir l'assurance qualité comme un outil stratégique pour la survie et le développement d'une entreprise.

L'intérêt pour le CESAG est qu'il constituerait une aide pour ses étudiants à la démarche d'élaboration d'une assurance qualité d'un système informatique et des risques pouvant affecter le système informatique.

Nous avons suivi un plan de travail structuré sur deux parties :

La première partie traitera, des aspects théoriques et comprendra trois chapitres qui seront répartis ainsi qu'il suit : nous débuterons le premier chapitre par une définition d'une politique de sécurité du système informatique. Puis un deuxième chapitre où nous ferons une étude des concepts généraux de l'assurance qualité d'une sécurité informatique et des méthodes mises en place pour son élaboration. Ceci nous permettra de nous situer dans l'idée générale du thème, par la définition des notions d'assurance qualité et de qualité de la sécurité informatique. Et enfin un troisième chapitre qui consistera à la méthodologie de recherche adoptée.

La seconde partie présentera l'aspect pratique et se composera de quatre chapitres : le premier concernera la présentation de Star Oil, un deuxième sur la stratégie de sécurité informatique de celui-ci, un troisième chapitre où nous procéderons à l'assurance qualité de la sécurité du

système informatique de la Star Oil et enfin on émettra des recommandations de sécurité complète dans le quatrième chapitre afin de pallier aux problèmes cités dans la première partie.

PREMIERE PARTIE :
CADRE THEORIQUE DE L'ETUUDE

Toute entreprise existante d'une certaine taille dispose en général d'un réseau informatique ; même celles qui n'en sont qu'à une idée de projet viable y pensent très souvent à une éventuelle mise en œuvre d'un réseau informatique au sein de leur future structure. La politique de sécurité du système informatique s'inscrit dans le système de management de l'organisme, donc de la sécurité des informations et processus. Elle constitue en effet le premier document à formaliser dans l'étape de planification et sera suivie des étapes de mise en œuvre, de vérification et d'amélioration du système de management de l'information.

Selon Riguidel (2003 : 56) « La réalisation de cette politique de sécurité va se concrétiser, par cette projection, d'une part sur les architectures et les technologies existantes et d'autre part sur les ressources informatiques disponibles. »

Qu'il s'agisse de données comptables, fiscales ou bancaires, le besoin en sécurité est essentiel en entreprise afin de crédibiliser le système, car l'impact éventuel des risques qui pourraient l'affecter peuvent avoir des répercutions dans toute l'organisation. Sa sécurité doit donc être mise en place de façon rigoureuse et être contrôlée régulièrement, tout en respectant à la fois les besoins des utilisateurs et des applications. La confiance des utilisateurs passe par la sécurisation des transactions, en utilisant par exemple le chiffrement, la signature électronique et les certificats. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs.

Nous présenterons cette première partie par la définition du système informatique, nous ferons ensuite une étude sur les menaces pouvant affecter le système informatique et nous achèverons cette partie par l'intérêt d'une sécurité du système informatique au sein de l'entreprise et de ses principaux acteurs.

Chapitre 1 : DEFINITION D'UNE POLITIQUE DE SECURITE INFORMATIQUE

Les systèmes informatiques (SI) gèrent des informations qui peuvent être convoitées par des individus dont le spectre s'étale du simple potache qui cherche à occuper son temps, jusqu'au professionnel chevronné du renseignement en passant par le criminel de droit commun, isolé ou dans une organisation. En proposant de nouveaux services et en traitant toutes sortes d'informations les SI constituent de nouvelles cibles qui ne sont pas toujours l'objet d'attentions adéquates de la part des dirigeants.

Les informations constituent une ressource stratégique, une matière première, elles sont un atout supplémentaire pour ceux qui les possèdent. La protection de ce patrimoine contre les malveillances doit par conséquent être un souci permanent d'organisation.

Il est nécessaire ainsi de décrire et d'illustrer de manière aussi complète que possible la sécurité informatique dans une entreprise.

1.1. Enjeux de la sécurité informatique au sein de l'entreprise

Plus aucune entreprise ne peut se passer de l'outil informatique, d'où la nécessité d'en assurer la sécurité et de la protéger contre les risques. Or, comme on ne se protège efficacement que contre les risques qu'on connaît, il importe de mesurer ces risques, en fonction de la probabilité ou de la fréquence de leur apparition et de leurs effets possibles. Chaque organisation a intérêt à évaluer, même grossièrement, les risques qu'elle court et les protections raisonnables à mettre en œuvre. Les risques et les techniques de sécurisation seront évalués en fonction de leurs coûts respectifs. Pour VOLLE (2004 : 21) « le système informatique est l'ensemble des moyens matériels et logiciels assurant le stockage, le traitement et le transport des données sous forme électronique ».

1.1.1. La sécurité informatique : Qu'est ce que c'est ?

Selon KALONJI BILOLO (2007 : 3) «la sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles ».

Elle consiste donc à protéger les informations contre la consultation abusive, la modification ou la destruction non autorisée et fournit les outils pour protéger l'information vitale de

l'entreprise et préserver ainsi son avantage compétitif. Elle permet ainsi de réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Cependant, aucune technologie ne peut à elle seule sécuriser l'information à 100%, il est nécessaire ainsi de combiner plusieurs contrôles, de mettre en œuvre différents moyens de protection et de les faire évoluer en même temps que les menaces. Le système informatique constitue un patrimoine essentiel des entreprises, constitué d'un ensemble de ressources matérielle et logicielle, il se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

La sécurité du système informatique cherche à apporter une meilleure maîtrise des risques qui pèsent réellement sur l'entreprise et répondre à certains enjeux qu'on peut résumer en quatre lettres « D.I.C.A » selon les termes de Eric Léopold et Serge Lhoste (2007 :30) « On a l'habitude de classer les risques en quatre grandes familles : disponibilité, intégrité, confidentialité et auditabilité. ». Une seule entrave à l'un de ces principes remet toute la sécurité en cause.

Figure 1 : Famille des risques

Source : Nous même, d'après l'approche MEHARI (Méthode Harmonisée d'Analyse de Risques).

- ✓ Disponibilité : garantir l'accès aux ressources, au moment voulu, aux personnes habilitées d'accéder à ces ressources ;
- ✓ Intégrité : garantir que les données échangées sont exactes et complètes ;
- ✓ Confidentialité : garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources de l'entreprise ;
- ✓ Auditabilité : garantir la traçabilité des accès et des tentatives d'accès et la conservation des ces traces comme preuves exploitables.

La sécurité informatique vise à inscrire l'évolution des systèmes dans le cadre d'un processus d'amélioration continue. La politique de sécurité du système informatique reflète donc la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information et de gestion de risques.

1.1.2. La sécurité informatique : Pourquoi ?

Outre les raisons évidentes liées au simple fait d'assurer la sécurité des informations, veiller rigoureusement à la sécurité informatique de sa structure est une nécessité qui peut naitre d'autres motivations principales telles que :

1.1.2.1. Les enjeux

Nous distinguerons trois types d'enjeux : les enjeux économiques, les enjeux politiques et les enjeux juridiques.

1.1.2.1.1. Enjeux économiques

Les organismes ou entreprises à but lucratif ont presque toujours la même finalité : c'est de réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information considéré comme moteur de développement de l'entreprise. D'où la nécessité de garantir la sécurité de ce dernier. La concurrence fait que des entreprises s'investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

Selon Éric Léopold et Serge Lhoste (2007 : 7), « Cette société, qui entre dans l'ère de l'information, a besoin de garantir la sécurité des données comme elle a toujours protégé les hommes et les biens contre les caprices de la nature et contre les autres hommes. »

Et d'après (GODART, 2002 : 16-17), «De manière plus concrète, une entreprise parle de sécurité pour protéger sa réputation, assurer la continuité de ses activités, protéger ses données stratégiques et ses propriétés intellectuelles, protéger les données privées de sa clientèle et de ses employés, se prémunir de la fraude, satisfaire aux exigences légales et éviter des pertes financières ».

1.1.2.1.2. Enjeux politiques

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du système d'information. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace.

1.1.2.1.3. Enjeux juridiques

Dans tout système d'information, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle ci doit se faire dans un cadre bien défini et dans le strict respect des lois en vigueur. En matière de juridiction, le non respect des lois et exigences relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise.

1.1.2.2. Les vulnérabilités

Tous les systèmes informatiques sont vulnérables, peu importe le niveau de vulnérabilité de ceux-ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire. Les vulnérabilités des systèmes peuvent être classés en catégorie (humaine, technologique, organisationnelle, mise en œuvre).

1.1.2.2.1. Vulnérabilités humaines

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit t'on pas souvent que l'erreur est humaine? Un système d'information étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le Système d'Information (SI).

Un exemple courant de vulnérabilité chez l'humain, c'est la surexploitation. Généralement, on a tendance à faire travailler un employé au delà de la limite de ses capacités normales. Ce qui peut l'amener à commettre des erreurs pouvant avoir des conséquences désastreuses pour l'entreprise.

1.1.2.2.2. Vulnérabilités technologiques

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine.

1.1.2.2.3. Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

1.1.2.2.4. Vulnérabilités relative à la mise en œuvre

Les vulnérabilités au niveau de la mise en œuvre peuvent être dues à la non prise en compte de certains aspects lors de la réalisation d'un projet.

1.1.2.3. Les menaces

Les systèmes informatiques sont confrontés aux menaces. Une menace est un événement pouvant se produire à tout moment et que l'on craint. Les menaces liées à la sécurité informatique se définissent par rapport à l'importance des différents types de systèmes informatiques dans le fonctionnement de l'entreprise. On peut dès lors désigner les différentes

menaces existantes et donc les objectifs à protéger. Les menaces encourus par l'entreprise peuvent être plus ou moins important selon les systèmes attaqués.

On peut distinguer ainsi deux types de menaces, les menaces stratégiques et les autres menaces mineurs.

1.1.2.3.1 Les menaces stratégiques

De nombreuses entreprises pratiquent la politique du zéro papier. Toute la « vie » de l'entreprise étant dans son système informatique, il est important que les serveurs garantissent d'une part l'intégrité et la confidentialité des données mais aussi un fonctionnement sans coupure qui entraînerait un ralentissement de l'activité. L'importance grandissante des échanges de données (E.D.I.) et du télétravail implique de même une fiabilité importante du système.

C'est ainsi que le vol, la destruction ou l'altération de données peuvent constituer des menaces importantes. C'est pourquoi, par exemple, la firme américaine Boeing dépensa 57 000 dollars pour vérifier des données après s'être aperçu de l'intrusion de 2 lycéens dans son système.

En effet, la modification de données peut constituer des menaces énormes en faussant le fonctionnement de l'entreprise. Une modification du moindre paramètre peut ainsi entraîner finalement la réalisation d'un produit fini défectueux.

De plus, l'espionnage industriel est devenu une réalité depuis que dès la fin de la guerre froide, les services de renseignements de la plupart des pays ont en partie reconverti leurs services sur l'intelligence économique (sans compter les initiatives privées). Certaines données comme par exemple les projets à long terme de l'entreprises, ou bien ses données commerciales, ou encore ses découvertes non encore brevetées sont bien souvent virtuellement possible à voler, étant donné que la plupart des systèmes même, d'une importance cruciale, sont reliés à internet (même le réseau SWIFT qui gère les transactions interbancaires est connecté), les menaces peuvent donc être considérables. Ces menaces sont donc à prendre en considération pour toutes entreprises, parce qu'ils peuvent entraîner une rupture dans la continuité de l'activité. Il existe aussi d'autres menaces, d'une importance moins stratégique, mais qui peuvent tout de même causer des troubles importants dans la vie de l'entreprise.

1.1.2.3.2 Les autres menaces

On peut distinguer au minimum deux autres types de cibles potentielles : le commerce électronique et les sites web.

En ce qui concerne le commerce électronique, il faut tout d'abord noter que ce risque peut être considéré comme stratégique pour une entreprise qui fonde son activité sur le télépaiement. Mais le télépaiement par internet offre beaucoup plus de failles, potentiellement exploitables par des pirates. La principale est bien sur la transmission des numéros de cartes bancaires et, pour certains systèmes, des codes. Le stockage de ces mêmes numéros est aussi un point faible, le serveur central pouvant faire l'objet d'une attaque visant à voler les fichiers de numéros.

Le piratage de sites web peut aussi constituer un risque. En effet ceux-ci constituent souvent la vitrine virtuelle d'une entreprise. Ces sites, n'ayant que rarement une importance stratégique pour l'entreprise, sont souvent peu protégés. C'est ainsi que des pirates détournent fréquemment de tels pages de leur but initial. La perte engendrée par une telle attaque s'évalue généralement en termes de perte d'image ou de crédibilité vis à vis des clients. Il faut noter que ces attaques peuvent être perpétuées dans deux situations : un pirate qui veut se faire un nom, ou l'attaque d'un groupe militant contre l'entreprise.

1.1.2.4. Les risques

Face aux différentes vulnérabilités susceptibles d'être exploitées pour attaquer les systèmes d'information et aux menaces multiformes existantes, il est clair que tout système d'information peut être impacté par des risques. Un risque est un événement susceptible de se produire.

Pour Didier Hallépée (2009: 35) « les risques sont les événements potentiels qui peuvent empêcher la réalisation des obligations contractuelles ou avoir des impacts importants sur la rentabilité, la pérennité ou la durée ».

Selon, HAMZAOUI (2005: 37), « le risque est un concept selon lequel la direction exprime ses inquiétudes concernant les effets probables d'un évènement sur les objectifs de l'entité dans un environnement incertain ». On peut classer les risques en plusieurs catégories dont voici quelques unes :

1. Accident ;
2. Perte ;
3. Vols ;
4. Fuites d'information.

1.1.2.4.1. Risque "accident"

Cette catégorie regroupe tous les sinistres comme les incendies, dégâts des eaux, explosions, catastrophes naturelles, etc. Certains de ces risques ne peuvent être raisonnablement pris en compte (par exemple, un effondrement causé par la présence d'une ancienne carrière souterraine), d'autres peuvent être prévenus ou combattus (par exemple, un incendie), l'informatique n'étant alors qu'un des aspects du problème.

Enfin, des mesures simples permettent de limiter les conséquences de certains accidents (par exemple, si la salle informatique est située au premier étage, on évitera la perte du matériel en cas d'inondation, même si celle-ci ne peut être combattue).

1.1.2.4.2. Risque "perte "

On range dans cette catégorie les coupures de courant, de télécommunications, les ruptures de stocks de fournitures essentielles, etc. Il existe des moyens permettant de palier à ces problèmes, notamment la redondance, les techniques statistiques et les alarmes.

1.1.2.4.3. Risque "vol"

Ces problèmes sont la plupart du temps marginaux, sauf dans les grandes entreprises, l'administration et les établissements d'enseignement où les vols ou dégradations sont généralement commis par les personnes fréquentant habituellement les lieux (personnel, étudiants). Ces problèmes sont loin d'être propres à l'informatique et les solutions existantes sont simples :

- ✓ installation d'alarmes et de dispositifs de télésurveillance ;
- ✓ fixation du matériel au mobilier et verrouillage des boîtiers ;
- ✓ utilisation de cartes internes pour les clés électroniques ;
- ✓ utilisation de matériel spécifique anti-vandalisme.

1.1.2.4.4. Risque "fuite d'information"

La fuite d'information est un phénomène difficile à éradiquer. Mais on peut en fonction des moyens dont on dispose, le rendre difficile à réaliser.

1.1.3. Comment la sécurité informatique est elle organisée ?

Les mécanismes de sécurité mis en place peuvent provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. Petites, moyennes et grandes entreprises s'exposent dans l'absolu aux mêmes risques si elles n'émettent pas de politique de sécurité adaptée, elle dicte la stratégie de sécurité de l'entreprise de manière claire et précise. Le fond et la forme sont donc primordiaux quelle que soit la nature de biens produits par l'entreprise, sa politique de sécurité doit satisfaire les points suivants :

- ***identification*** **:** information permettant d'indiquer qui vous prétendez être. Une identification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique. Une identification plus évoluée peut être le relevé d'empreinte digitale, l'analyse faciale, rétinienne bref les méthodes biométriques ;
- ***authentification*** **:** information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être. Une authentification élémentaire est le mot de passe que vous entrez. Une authentification forte combine une chose que vous possédez, une chose que vous connaissez (code personnel par exemple) et une chose que vous savez faire (par exemple une signature) ;
- ***autorisation*** **:** information permettant de déterminer quelles seront les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé aura accès ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise ;

- ***confidentialité* :** ensemble des mécanismes permettant qu'une communication de donnée reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données ;
- ***intégrité :*** ensemble des mécanismes garantissant qu'une information n'a pas été indûment modifiée ;
- ***disponibilité* :** ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles pour qui a droit, que ces dernières concernant l'architecture réseau, la bande passante, le plan de sauvegarde ... ;
- ***non répudiation* :** mécanisme permettant de garantir qu'un message ne peut être renié par son émetteur ;
- ***traçabilité* :** ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. Il est nécessaire ainsi de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- ✓ identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- ✓ élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- ✓ surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- ✓ définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

1.2. Objectif d'une politique de sécurité informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

1.2.1. Principes généraux d'une politique de sécurité informatique

La sécurité d'un système est un ensemble de moyens techniques, organisationnels, juridiques et humains, nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un système d'information englobe celle du système informatique sur lequel il s'appuie. Afin d'éviter un certain nombre d'écueils classiques, une politique de sécurité réseau doit respecter un ensemble de principes génériques.

Ces principes permettent notamment à chacun de bien cerner les enjeux, de la rédaction d'un document de politique de sécurité, qui n'est pas un document comme les autres. Un document de politique de sécurité peut être écrit de plusieurs manières, allant d'un texte unique à une infrastructure de politique de sécurité. Le choix d'écrire un ou plusieurs documents est le plus souvent dicté par la taille de l'entreprise. Plus l'entreprise est importante, plus il est intéressant de créer des documents séparés, chaque niveau faisant référence au niveau supérieur. La mise en place de la politique de sécurité du système informatique est le contraire de l'improvisation: il faut préétablir ce que l'on doit faire, le faire et apporter la preuve que cela a été fait. Pour créer cette confiance, on prend appui sur un nombre restreint de textes écrits, précisant les règles et les procédures, qui constituent le système documentaire de l'assurance de la qualité.

Tableau 1 : La politique de sécurité informatique

POLITIQUE DE SECURITE		
Outils	**Personnes**	**Procédures**
-chiffrement -filtrage -contrôle d'accès -périrnètre de sécurité	-sensibilisation -formation -contrôle -surveillance	-gestion - contrôles -évaluation Suivi -mise à jour
Champs d'application		**Législation**
-systèmes -données -Réseaux - programmes -environnement physiques -environnement énergétiques		-contraintes légales -contraintes juridiques

Source : Nous même, à partir de CARPENTIER (2009:34).

1.2.2. Niveaux d'une politique de sécurité informatique

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue. Selon Securiteinfo (2004), « nous pouvons avoir 7 classes de fonctionnalités, ce qui nous donne dans l'ordre croissant D, C1, C2, B1, B2, B3, A1 » :

1.2.2.1. Le niveau de sécurité D

Il correspond à un niveau de sécurité minimal, ce qui veut dire aucune contrainte, on y retrouve le système DOS.

1.2.2.2. Le niveau de sécurité C1

Il correspond à un niveau de protection discrétionnaire. C'est à dire que l'on assure la séparation des utilisateurs et des données avec la notion de sujet et d'objet, que l'on contrôle l'accès aux informations privées et que les utilisateurs coopèrent sur le même niveau de sensibilité.

1.2.2.3. Le niveau de sécurité C2

Ce niveau offre un accès contrôlé. C'est à dire que l'on affine le contrôle d'accès, au moyen du login et de l'audit. De plus, on sépare les ressources à protéger. Le passage de la classe C (protection discrétionnaire) à la classe B (protection mandataire) se fait par le biais de la labellisation des données.

1.2.2.4. Le niveau de sécurité B1

Il offre ainsi une protection par labellisation. On a donc une politique de sécurité associée au marquage des données et au contrôle obligatoire des sujets et des objets.

1.2.2.5. Le niveau de sécurité B2

Pour atteindre ce niveau dit "Protection Structurée", il faut renforcer le contrôle d'accès, ne pas disposer de canaux cachés, avoir une authentification renforcée, avoir des contraintes

accrues de gestion et de contrôle de la configuration ainsi que disposer d'une TCB (Trusted Computing Base) fondée sur un modèle défini et documenté

1.2.2.6. Le niveau de sécurité B3

C'est le niveau de " domaine de sécurité ", il faut obligatoirement un administrateur de sécurité, un audit accru et la TCB intervient lors de tout accès de sujet à objet, doit résister à l'intrusion et doit pouvoir être analysée et testée.

1.2.2.7. Le niveau de sécurité A1

Ce niveau est celui dit de "conception vérifiée". Comme son nom l'indique, il impose d'avoir une FTLS (Formal Top Level Specification) pour la conception de la TCB et du modèle. Il impose en plus des contraintes sur la gestion de la configuration et un administrateur de sécurité et du système distinct.

1.2.3. Les différents types de politiques de sécurité

Nous pouvons considérer que la sécurité informatique est divisée en deux grands domaines :

1.2.3.1. La sécurité organisationnelle

Elle concerne la politique de sécurité d'une société (code de bonne conduite, méthodes de classification et de qualification des risques, plan de secours, plan de continuité…).

Le périmètre de la sécurité est très vaste :

- ✓ la sécurité des systèmes d'information ;
- ✓ la sécurité des réseaux ;
- ✓ la sécurité physique des locaux ;
- ✓ la sécurité dans le développement d'applications ;
- ✓ la sécurité des communications ;
- ✓ la sécurité personnelle.

Une fois la partie organisationnelle traitée, il faut mettre en œuvre toutes les recommandations, et plans dans le domaine technique de l'informatique, afin de sécuriser les réseaux et systèmes : cet aspect relève de la sécurité technique.

1.2.3.2. La sécurité technique

Elles assurent la disponibilité (les services et les informations doivent être accessibles aux personnes autorisées quand elles en ont besoin et dans les délais requis), l'intégrité (les services et les informations ne peuvent être modifiés que par les personnes autorisées), et la confidentialité (l'information est accessible uniquement à ceux qui y ont droit). Les techniques de sécurisation d'un système incluent :

- ✓ les vulnérabilités du système ;
- ✓ la sécurité des données: chiffrement, authentification, contrôle d'accès ;
- ✓ la sécurité du réseau: pare-feu ;
- ✓ la surveillance des informations de sécurité ;
- ✓ l'éducation des utilisateurs ;
- ✓ le plan de reprise des activités.

D'après Laurent Bloch, et Christophe Wolfhugel (2009 : 89) «Le système ou le pare-feu qui protège, c'est celui pour lequel il y a sur le site un ingénieur (oui, un ingénieur, les gens qui savent faire ça sont des ingénieurs) ».

1.3. Les acteurs de la sécurité informatique

Il est essentiel de faire une étude sur les acteurs de cette sécurité informatique.

1.3.1. Responsabilité de la Direction Générale

La politique de sécurité informatique reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information et de gestion des risques de manière générale. Celle ci décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme conçu par ses principaux acteurs. La validation de la politique de sécurité informatique par la direction traduit la reconnaissance officielle accordée à la sécurité de son système. Elle informe ainsi les tiers sur la maîtrise des enjeux tout en éclairant sur les choix en termes de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information de l'entité. La direction générale est la première responsable de la sécurité de l'informatique au sein de l'établissement. Elle s'assure que les valeurs et les orientations en matière de sécurité de soient partagées par

l'ensemble du personnel. Selon Éric Léopold & Serge Lhoste, (2007 : 103) « La politique de sécurité informatique est l'aboutissement et la synthèse de ces travaux. Elle ne peut être définie que si l'ensemble des parties intéressées coopère. Bien sûr, l'avis des administrateurs, qui ont la responsabilité au jour le jour des ressources, est essentiel. Pourtant, il ne faut pas négliger d'associer au processus de définition de la politique de sécurité informatique les organes de décision, qui seuls auront les pouvoirs de mettre en place effectivement les recommandations».

Ainsi, il ne revient pas au responsable informatique de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers, la direction générale approuve la politique et s'assure de sa mise en œuvre. À cet égard, il autorise et approuve la politique de sécurité et toutes les directives sous-jacentes. Le soutien de la direction sera d'autant plus important que les progrès réalisés par la démarche de l'assurance qualité pourront être mesurés. À cette fin, elle :

- ✓ s'assure de l'application de la politique dans l'organisation;
- ✓ apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique;
- ✓ reçoit périodiquement un rapport du responsable de la sécurité de l'information sur l'application de la politique;
- ✓ exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

1.3.2. Le responsable de la sécurité informatique

Sous l'autorité immédiate du directeur général, le responsable de la sécurité informatique gère et coordonne la sécurité informatique au sein de l'entreprise. Il doit donc harmoniser l'action des divers acteurs dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité informatique.

Selon REIX (2005 : 486) « désigné par la Direction Générale, le responsable de la sécurité du système d'information (RSSI) ou le responsable du système informatique (RSI) est le maitre d'œuvre de la politique de sécurité informatique ». Le responsable de la sécurité informatique doit être en mesure de donner un service de qualité, un savoir-faire expert et un soutien pratique et efficace dans toutes les activités reliées à la sécurité informatique. Il veille

à ce que les installations des programmes et les logiciels de même que les recommandations faites aux utilisateurs soient conformes aux normes, aux standards et aux audits concernant la sécurité du système. Il peut aussi être appelé à tester et à vérifier des appareils et des instructions mis en place pour assurer la sécurité des systèmes d'informations. La sécurité informatique revêt aujourd'hui une telle importance que les responsables de la sécurité des systèmes d'informatique sont couramment rattachés aux directions générales des entreprises. La mission du responsable informatique est effectivement essentielle puisqu'il a la charge des choix et des actions relatives à la sécurité des systèmes, des réseaux, des applications et des données de l'entreprise. C'est à lui qu'incombe également la responsabilité de mettre en place les plans de continuité et de reprise d'activité après sinistre qui garantiront la bonne marche de l'organisation.

Ses responsabilités sont de :

- ✓ veiller à la qualité des produits et des services informatiques selon les standards, les normes et les procédures en vigueur ;
- ✓ résoudre les problèmes encourus de façon proactive, prévoir les risques et apporter les solutions requises ;
- ✓ analyser et comprendre les besoins de l'entreprise cliente en matière de sécurité d'informations ;
- ✓ conseiller les personnes responsables de la sécurité des programmes, des logiciels et des systèmes d'informations et leur faire les recommandations nécessaires ;
- ✓ participer au développement, à la mise en place et à la réalisation des stratégies en matière de sécurité et de gestion des risques ;
- ✓ mettre en place un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- ✓ connaitre les standards et les normes d'architecture et établir des procédures d'utilisation du réseau par les utilisateurs afin qu'il demeure sécurisé ;
- ✓ définir un plan de reprise après incident…

Par ailleurs le rôle du responsable informatique est de faire en sorte que les ressources informatiques et les droits d'accès à celles-ci soient en cohérence avec la politique de sécurité retenue par la direction générale. De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de la conseiller sur les stratégies à mettre en œuvre, ainsi que d'être

le point d'entrée concernant la communication aux utilisateurs des problèmes et recommandations en terme de sécurité. La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation de la direction auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- ✓ la sensibilisation des utilisateurs aux problèmes de sécurité ;
- ✓ la sécurité logique, c'est-à-dire la sécurité au niveau des données ;
- ✓ la sécurité des télécommunications ;
- ✓ la sécurité des applications ;
- ✓ la sécurité physique, soit la sécurité au niveau des infrastructures matérielles.

Conclusion

La sécurité est un enjeu majeur des technologies numériques modernes. Avec le développement de l'internet et de la notion du partage en général, les besoins en sécurité sont de plus en plus importants. Le développement d'applications Internet telles que le commerce électronique, les applications médicales ou la vidéo conférence, implique de nouveaux besoins comme, l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, etc.

Chapitre 2. CONCEPTS GENERAUX DE L'ASSURANCE QUALITE D'UNE POLITIQUE DE SECURITE INFORMATIQUE

Après avoir précisé ce qu'est une politique de sécurité informatique, il est maintenant important d'effectuer une assurance qualité de ce système. Pour ce faire nous allons définir la notion d'assurance qualité, les méthodes d'élaboration de celle-ci. Et enfin on mettra en place quelques modèles et stratégies d'assurance qualité.

2.1. Qu'est ce que l'assurance qualité ?

L'assurance de la qualité est selon l'organisation CNUCED/OMC (1996 : 7) « l'ensemble des activités préétablies et systématiques mises en œuvre dans le cadre du système qualité et démontrées en tant que besoin, pour donner la confiance appropriée en ce qu'une entité (service, produit, processus, activités ou organisation) satisfera aux exigences en matière de qualité ».

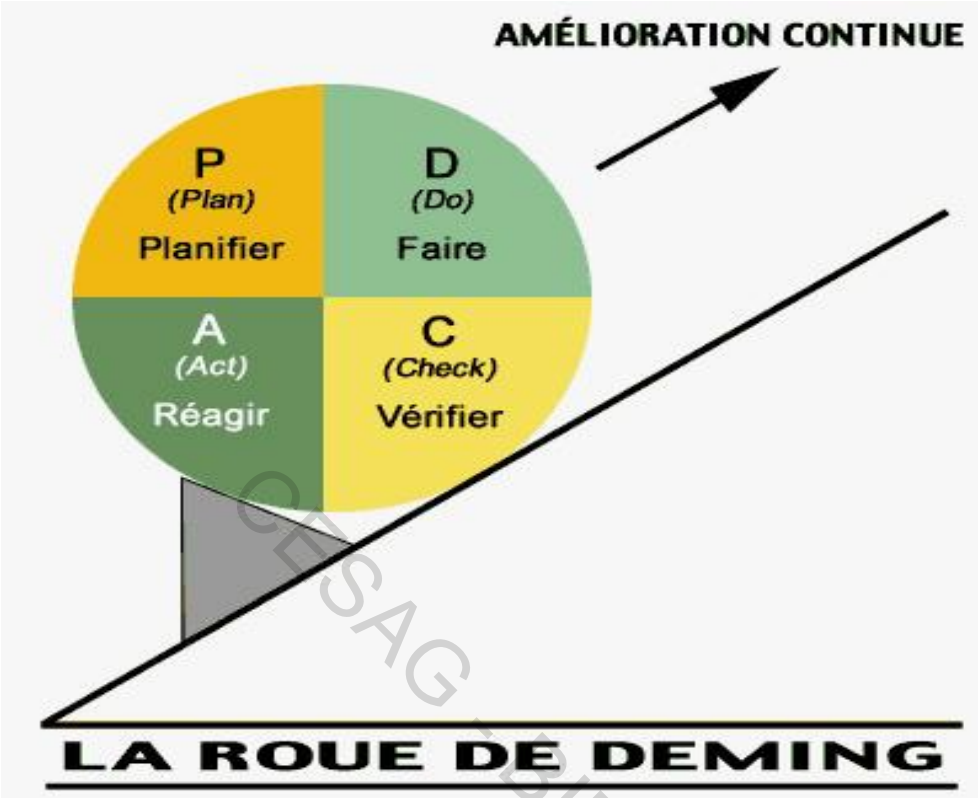
A travers la norme ISO 9000 on l'a définie comme étant « l'ensemble systématique et planifié d'actions nécessaires pour fournir une confiance adéquate dans le fait que le processus de développement ou de maintenance du système est conforme aux besoins fonctionnels et managériaux, respectant le planning et les contraintes budgétaires ».

En termes opérationnels, assurer la qualité, c'est définir et mettre en œuvre les dispositions propres à fonder cette confiance aux yeux de l'entreprise elle-même (assurance interne de la qualité), mais aussi aux yeux des tiers (assurance externe de la qualité).

En termes d'objectifs, l'utilisateur veut avoir l'assurance de la qualité, c'est-à-dire la confiance appropriée en ce que la qualité voulue sera obtenue ; l'entreprise doit acquérir elle-même cette confiance et en procurer les fondements.

L'Assurance Qualité d'un système est donc l'ensemble de l'organisation, des responsabilités, des procédures, processus et moyens nécessaires pour mettre en œuvre le management de la qualité.

Figure 2 : Roue de Deming



Source : L'encyclopédie libre Wikipédia.

2.1.1. Définition de la notion de qualité

Bien souvent, le terme « qualité » est interprété de manières très diverses, dans le langage courant, la qualité est synonyme de satisfaction. Pour l'entreprise en revanche, la qualité implique par exemple le respect de la performance spécifiée (respect de l'environnement et sécurité). Pouvant être ambigu, vue sa multiplicité de sens, sa définition a toutefois été précisée au niveau de l'OIN (Organisation Internationale de Normalisation). Selon l'OIN (2000 : 7) ; « la qualité est l'aptitude d'un ensemble de caractéristiques intrinsèques à satisfaire des exigences ».

2.1.2. Principal objectif de la mise en place d'une assurance qualité

L'importance de posséder un système informatique sécurisé est vitale pour une entreprise. Partis de ce postulat, les managers doivent rechercher des procédés visant à garantir à la fois la qualité et la régularité du système afin d'assurer ses performances. L'entreprise sera amenée à mettre en place dans ce cas l'Assurance Qualité du système informatique.

Pour que cette démarche soit efficace, elle doit s'appliquer à tous les groupes concernés par le fonctionnement de l'organisation : les dirigeants, les salariés. Ce concept d'Assurance Qualité sert à la fois des objectifs internes et externes :

En interne, l'Assurance Qualité vise à donner confiance en sa stratégie à la direction avec la baisse des anomalies significatives et maintenir le niveau de compétence de l'entreprise et en externe elle permet d'obtenir la confiance des tiers. Elle permet en outre d'assurer un niveau acceptable de confiance dans la conformité du système de sécurité informatique, aux spécifications fonctionnelles.

2.2. Les grandes étapes de la mise en œuvre d'un processus d'assurance qualité

Comme dit plus haut, l'assurance qualité n'est pas un modèle unique et prêt à l'emploi. Néanmoins, elle peut suivre les lignes principales de démarches existantes ou ayant déjà fait des preuves. L'élaboration de l'assurance qualité d'une sécurité informatique doit reposer sur une approche méthodologique par une identification des priorités, l'implication des acteurs clés et une analyse des risques. Le recours aux normes et procédés existantes est nécessaire tant sur le plan de l'élaboration que celui de sa mise en œuvre.

2.2.1. Identifications des priorités

De façon pratique, la mise en œuvre de l'assurance qualité dans une entreprise peut être conduite en quatre grandes phases à savoir : une réflexion préalable, un cadrage des idées, le lancement de la démarche et le pilotage des actions.

2.2.1.1. Engager une réflexion préalable

Il s'agit d'un préalable essentiel à tout projet d'entreprise. Il convient, bien évidemment, que la direction du service soit claire sur les enjeux tactiques et sur sa volonté de s'engager dans une telle démarche, ainsi que sur sa finalité. Cet engagement doit se manifester concrètement dans les faits, et ne pas se limiter à quelques exhortations faites lors des assemblées ou à des articles signés du directeur dans les supports de communication interne. Une démarche d'assurance qualité est un processus de changement profond et progressif.

L'engagement de la direction sous-tend qu'elle ait bien pris conscience de la nécessité de lancer une telle démarche pour répondre aux enjeux du service et des implications que cela

représente en termes de priorités, de moyens nécessaires, de temps et d'énergie à y consacrer. L'engagement de la direction doit être issu d'un travail spécifique en équipe de direction. Tout d'abord, il importe de s'accorder sur le sens donné à la qualité, de sensibiliser les membres de la direction aux concepts et enjeux de la qualité, de partager des références communes et de parler le même langage. A l'occasion de cette sensibilisation, les enjeux et la finalité de la démarche doivent être identifiés.

2.2.1.2. Définir le cadre de mise en œuvre de la démarche

Après clarification et partage de la finalité, puis validation de l'engagement de la direction, la démarche reste à bâtir. Il s'agit ici de définir :

- ✓ les types d'actions à lancer, le secteur et les moyens d'y parvenir ;
- ✓ la façon de piloter la démarche ;
- ✓ les moyens matériels et humains à dégager pour assurer sa mise en œuvre ;
- ✓ la communication à mettre en place pour accompagner la démarche ;
- ✓ les formations à engager et les personnes concernées.

Les réponses à ces différentes préoccupations sont issues des premières réflexions conduites en comité de direction. L'organisation d'un séminaire des cadres permet, tout en diffusant des références communes, de valider la faisabilité de démarches de l'assurance qualité, de définir plus précisément les domaines de démarrage et les personnes volontaires, et d'établir un projet global portant sur les différents aspects de la démarche.

A cette occasion, les messages explicitant et justifiant l'engagement de telles démarches, leur articulation avec les démarches déjà engagées, le sens qu'on leur donne, les résultats qu'on en attend, l'appui qui sera donné aux acteurs doit être bien précisé. Quels que soient les qualificatifs donnés à ces démarches, il est indispensable d'en expliciter clairement et avec pédagogie les enjeux, le sens et la finalité : c'est la condition de l'engagement et de l'adhésion du personnel. A ce stade, la communication est plus qu'indispensable, pour favoriser l'appropriation par le personnel de la finalité de la démarche et une analyse des risques.

2.2.1.3. Organiser et lancer les premières actions qualité

Ces actions, qui peuvent prendre des formes diverses, visent à améliorer la qualité de la sécurité du système informatique. Elles s'appuient sur des méthodes, des outils, voire des

dispositifs organisationnels, amélioration des processus, implication du personnel et mesure. Selon les circonstances, les actions portent plus particulièrement sur l'un ou l'autre de ces aspects. Néanmoins, on doit veiller à ce que, peu à peu, l'ensemble des points soit pris en compte, faute de quoi, l'action ne serait pas de « bonne qualité ».

2.2.1.4. Organiser et assurer le pilotage

Au fur et à mesure de l'avancement des actions, puis de leur évaluation, la démarche est réorientée. Des actions supplémentaires sont lancées, des dispositifs sont étendus ou systématisés. La démarche s'étend dans ses modalités d'actions et dans son champ d'intervention, l'assurance qualité se construit. La communication et la formation continuent à accompagner le processus.

La démarche se développe d'une façon plus autonome, en étant portée progressivement par tous les agents du service et notamment l'encadrement. Pour assurer la cohérence entre les actions et veiller à leur pertinence, un pilotage efficace doit être organisé. Ce pilotage repose :

- ✓ d'une part, sur le développement d'un système global, organisé et formalisé, qui intègre toutes les actions qualité et permet leur suivi. On parle de pilotage opérationnel ;
- ✓ d'autre part, sur la mesure et l'évaluation des résultats, la veille externe et la connaissance de l'évolution des attentes des différents clients. On parle de pilotage stratégique.

Le dispositif de pilotage joue un rôle majeur. Pour bien fonctionner, il doit reposer sur un système d'information et de communication efficace entre le dispositif de pilotage et l'ensemble du service.

2.2.2. Définition et rôle des principaux acteurs de l'assurance qualité

2.2.2.1. Le responsable qualité

Il doit offrir son savoir-faire durant tout le processus. Elle doit s'assurer de la qualité à toutes les étapes (de la conception à la documentation) des équipements et des logiciels. Le directeur qualité doit garantir l'efficacité des techniques d'assurance qualité en vigueur dans les conditions définies, pour cela il doit :

- ✓ veiller à la procédure de contrôle des conditions de fonctionnement des différents outils informatiques ;
- ✓ veiller à la qualité des produits et des services informatiques selon les standards, les normes et les procédures en vigueur ;
- ✓ participer au développement, à la mise en place et à la réalisation des stratégies en matière d'assurance qualité et de la gestion des risques ;
- ✓ conseiller les personnes responsables des systèmes d'information et leur faire les recommandations appropriées ;
- ✓ élaborer et appliquer des solutions aux défaillances informatiques ;
- ✓ être en mesure d'analyser les coûts des systèmes informatiques, les coûts de leur utilisation et des solutions proposées pour l'optimisation ;
- ✓ disposer des compétences requises ;
- ✓ connaître la gestion de la qualité et la gestion des risques ;
- ✓ savoir gérer les imprévus tout au long des projets ;
- ✓ connaître les logiciels appropriés ;
- ✓ connaître les standards, les normes et les procédures et être capable de faire respecter l'utilisation de ses applications et ses adaptations par les utilisateurs ;
- ✓ comprendre les demandes des clients et être apte à répondre à leurs attentes ;
- ✓ comprendre l'utilisation du matériel utilisé : progiciels, outils de bases de données.

2.2.2.2. Les autres acteurs de l'assurance qualité

- ✓ Directeur Général : Établit les procédures (plan d'assurance qualité, manuel de procédures, etc.) au niveau de l'entreprise ;
- ✓ Ingénieur qualité : Représente le directeur qualité au sein d'une entité Garant de la bonne application des procédures ;
- ✓ Auditeur : Définit les méthodologies pour l'amélioration de la qualité et du système de management de la qualité ;
- ✓ Contrôleur qualité : Évalue la qualité du produit ou du service et supervise toutes les actions que l'on peut entreprendre.

2.2.3. Analyse des risques

Le système informatique d'une entreprise, à l'instar de tout système de gestion d'entreprise complexe, est composé de différentes parties, qui ont une importance plus ou moins stratégique. Les moyens employés pour protéger ces divers composants doivent donc être en adéquation avec leur importance. Le choix des dispositifs de protection est l'aboutissement d'une démarche rationnelle d'analyse des risques. Celle-ci prend en compte d'une part les caractéristiques du dispositif à protéger (valeur pour l'entreprise) et d'autre part les probabilités de concrétisation des différentes menaces.

Ainsi, divers facteurs doivent être pris en compte lors de la rédaction du rapport de l'analyse des risques, notamment : le coût des mesures de sécurité proposées par rapport aux coûts de l'absence de mesures de sécurité, la fréquence réelle de chaque catégorie d'infractions à la sécurité, la question de savoir si une infraction cause des dommages évidents, la valeur des dommages causés par une catégorie particulière d'infractions à la sécurité, la valeur non monétaire des dommages (quelle valeur faut-il attribuer à la communication non autorisée de renseignements personnels, à l'intérêt national, à la perte d'un client ou de la confiance du public, difficulté à déceler certaines catégories d'infractions à la sécurité, la difficulté à prévenir certaines catégories d'infractions à la sécurité et la possibilité de dommages considérables qui ne risquent guère de survenir, par rapport à la possibilité de dommages moindres qui risquent davantage de survenir).

Un risque se définit comme une combinaison de menaces exploitant une vulnérabilité et pouvant avoir un impact. De manière générale, les risques sont soit des causes (attaques, pannes, …) soit des conséquences (fraude, intrusion, divulgation …). On peut résumer une démarche d'analyse des risques informatiques en 8 étapes :

1. Identifier ce qu'il faut protéger ;
2. Identifier les menaces ;
3. Identifier les points faibles ;
4. Estimer la probabilité des risques.

2.3. Méthodes et normes d'élaboration de l'assurance qualité

Afin de mener la mission d'assurance qualité de manière professionnelle et efficace, il est

important de s'appuyer sur des normes, des standards, des référentiels de bonne pratique ou des méthodes spécifiques. Il existe de nombreux référentiels sous différentes formes, il peut s'agir de normes nationales ou internationales, de bases de connaissances, d'outils méthodologiques, de réglementations. Le recours à ces catalogues peut s'avérer utile pour garantir une bonne complétude des règles de sécurité.

2.3.1. Model d'assurance qualité

Afin de s'assurer que le système de sécurité informatique répond parfaitement aux exigences préétablies, différentes actions peuvent être réalisées:

2.3.1.1. Les mesures

Engagement de la direction et sensibilisation des salariés (définition de la politique qualité). Mise en place d'un comité de pilotage. Le comité définit les priorités et se charge du suivi de la démarche d'assurance qualité. Il a un rôle de facilitation : désignation du responsable de l'assurance qualité sécurité informatique (fonction de formation/animation). Selon DURET D. & PILLET M (2002 : 354) « *Que chacun fasse de son mieux, n'est pas suffisant. Il était nécessaire que les gens aient connaissance des objectifs à atteindre. Des transformations drastiques sont indispensables. La responsabilité du changement repose entièrement et uniquement sur les épaules des Directions d'entreprises. La première étape est d'apprendre comment changer*. »

La mesure du bon déroulement des procédures de sécurité informatique à travers la réalisation d'un diagnostic : étape préalable à toute action. Etat des lieux, évaluation du système de sécurité, (visite des lieux, mise en évidence des éléments qui répondent déjà aux exigences et des disfonctionnements, évaluation des différents coûts) ;

Rédaction d'un manuel d'assurance qualité, plan d'action/d'amélioration : définition du dispositif d'accompagnement (choix des processus et des objectifs), mise en forme du plan d'action (qui fait quoi), définition d'indicateurs de qualité

La mesure de la conformité et de l'efficacité du système de sécurité informatique s'effectue à travers des audits internes planifiés annuellement. Mise en œuvre des processus, réalisation des procédures (techniques, organisationnelles, relationnelles et managériales) définies par le

Comité de Pilotage- Suivi et gestion, opération de contrôle qualité, examens réguliers des indicateurs qualité, recherche d'amélioration continue, audits blancs, démarche préliminaire pour un audit de certification.

2.3.1.2. Les contrôles et essais

L'objectif visé est de vérifier la conformité du système par rapport aux spécifications et standards, de faire des corrections le cas échéant. Ces contrôles sont réalisés par le service informatique.

Voici quelques éléments pouvant servir de base à un contrôle :

- ✓ Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- ✓ Quel est le coût et le délai de remplacement ?
- ✓ Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Et enfin faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs ...).

2.3.1.3. Enregistrement des contrôles

L'enregistrement des contrôles et essais permet de vérifier que l'ensemble des contrôles a été effectué et que les résultats ont satisfait ou non la conformité aux exigences spécifiées.

2.3.1.4. Analyse des données et amélioration continue

L'ensemble des données recueillies à travers les mesures et contrôles faites sus mentionnés est soumis à une analyse, afin de dégager les pistes prioritaires d'amélioration du système.

On recueille un ensemble de données du système de sécurité en vue de les analyser. Les analyses donnent lieu à des actions correctives et préventives pour l'amélioration continue de ses performances.

L'état des contrôles et essais est identifié par des moyens appropriés, afin d'indiquer la conformité ou la non-conformité du système par rapport aux analyses effectués. En cas d'urgence, les anomalies sont repérées, et doivent être retirés à tout moment.

Les analyses effectuées concernent :

- ✓ les données de la maintenance ;
- ✓ les risques internes et externes ;
- ✓ l'évolution des risques.

Ainsi, peut-on présenter tout ce qui a été avancé, concernant l'assurance qualité de la sécurité informatique, sous forme d'un schéma récapitulatif :

- **Préétablir**

- ✓ fixer la politique et les objectifs
- ✓ définir les responsabilités
- ✓ décrire les règles pour assurer la maîtrise de la qualité
- ✓ formaliser ces règles (MNQ procédures, plan qualité, instructions, etc...

- **Prouver**

Enregistrer les résultats relatifs à la qualité (mesures, indications, audits, enregistrements)

- **Pratiquer**

- ✓ former.
- ✓ mettre en œuvre les règles.
- ✓ auto-contrôler.
- ✓ auditer.
- ✓ communiquer.

- **Progresser**

- ✓ exploiter les résultats.
- ✓ améliorer la maîtrise de son savoir- faire.
- ✓ actualiser régulièrement le système informatique.
- ✓ maîtriser son système informatique.

Tableau 2 : Exemple d'identification des risques

Source	FAIBLESSES apparentes	RISQUE détecté		RISQUE OPERATIONNEL	REPONSES (réponse contradictoire, solution proposée, palliatif retenu)	RECOMMANDATIONS
		(O/N)	Nature du risque	POUR STAR OIL		
Narratif		O				

Source : Nous même.

2.3.2. Les Normes internationales ISO

L'Organisation Internationale de Normalisation (ISO) est une fédération d'organismes nationaux de normalisation fondée en 1947 et comprenant plus de 140 pays. A ce jour, l'ISO a élaboré près de 10 000 normes internationales volontaires, sur la base du consensus, dans presque tous les domaines de l'activité industrielle, économique, scientifique et technique. Les plus connues et reconnues dans le domaine de l'assurance qualité sont les normes ISO 9000 de l'Organisation International de Normalisation.

ISO 9000 a pour objectif premier d'aider les entreprises dans leur recherche de la qualité et d'y parvenir de manière optimale, par la prévention des erreurs. ISO 9000 fixe des lignes directrices pour diriger, coordonner et contrôler chacune des activités d'assurance qualité menées dans une entreprise. Elle décrit les principes essentiels des systèmes de management de la qualité et en spécifie la terminologie.

Tandis que la norme ISO 9001 énonce les exigences auxquelles doit satisfaire une démarche qualité, elle n'impose pas de modalités quant aux moyens d'y parvenir. Elle laisse donc une marge de manœuvre et une flexibilité considérable d'application dans les différents secteurs économiques et leurs environnements de travail, et dans des cultures nationales différentes.

Une entreprise qui satisfait aux exigences d'ISO 9000 doit procéder à un audit de son système qualité. L'entreprise peut aussi faire appel au service d'un organisme indépendant de

certification de la qualité, pour obtenir un certificat de conformité à l'ISO 9000. Cette dernière option est devenue très populaire dans le monde des entreprises étant donnée la crédibilité que revêt une évaluation indépendante.

Les normes ISO 9000 sont révisées périodiquement afin de mieux faire face aux contraintes, très évolutives de l'environnement et de répondre ainsi à leurs attentes. Depuis la version ISO 9000 de 1994, la dernière révision de cette norme date de 2000 ; d'où la notation « ISO 9000 : 2000 ».

Une autre norme reconnue internationalement est la norme ISO 17999 "code of practice for information security management", c'est-à-dire le code de bonne pratique pour la gestion de la sécurité de l'information. Cette norme est un référentiel de bonnes pratiques de sécurité et des contrôles liés à leurs applications.

La norme ISO 17999 est apparue en 2000 dans le monde de la sécurité des systèmes 'information. Elle est destinée aux dirigeants, aux directeurs de système d'information et aux responsables sécurité (Chief Security Officer, RSSI). Elle a été définie afin de répondre au besoin d'un "label de confiance" d'un organisme reconnu internationalement.

Tout comme la norme ISO 9000, bien connue de tous dans le domaine de la qualité, la norme ISO 17999 a pour objectif d'établir un label de confiance reconnu de tous en ce qui concerne la sécurisation de l'information sous un aspect global.

Les échanges de données nationales et internationales entre collaborateurs d'une même organisation, partenaires et clients couplés aux TIC impliquent la nécessité de s'accorder sur une norme pouvant aider à sécuriser l'information et les processus d'échanges. La norme ISO 17999 propose un ensemble de mesures organisationnelles et techniques, mais n'impose pas de solution technologique particulière.

Cette norme accorde une importance particulière à certains aspects cruciaux de la sécurité :

- ✓ le support des dirigeants quand à la mise en œuvre d'une politique de sécurité et la détermination des moyens humains à y associer ;
- ✓ l'identification des menaces propres à l'organisation et l'évaluation des risques associés;

- ✓ la classification des informations afin de ne déployer les moyens que sur celles qui le nécessitent ;
- ✓ les dispositions à mettre en œuvre afin d'instaurer une "culture sécurité".

Nous pouvons citer en outre quelques autres normes ISO liées à la sécurité informatique telles que :

- **ISO 13335:**
    - concepts et modèles pour la gestion de la sécurité des TIC ;
    - techniques pour la gestion des risques relatifs à la sécurité des TIC ;
    - techniques pour la gestion de sécurité IT ;
    - sélection de sauvegarde ;
    - guide pour la gestion de sécurité du réseau…
- **ISO 14001 :** repose sur le principe d'amélioration continue de la performance environnementale par la maîtrise des impacts liés à l'activité de l'entreprise. Celle-ci prend un double engagement de progrès continu et de respect de la conformité réglementaire. La roue de Deming est le principe de base sur lequel reposent toutes les exigences de la norme ISO 14001. Cette dernière est d'ailleurs architecturée selon la spirale d'amélioration continue :
    - Préétablir : Formaliser et écrire les procédures de travail ;
    - Pratiquer : Dérouler l'action conformément aux procédures ;
    - Prouver : Démontrer que l'action s'est déroulée comme prévue ;
    - Progresser : Corriger l'action en vue d'amélioration.
- **ISO 14516:** lignes directrices pour l'utilisation et la gestion des services de tiers de confiance ;
- **ISO 15408:** critères d'évaluation de la sécurité des TIC ;
- **ISO 18044:** gestion d'incidents de sécurité de l'information…

En outre la gestion des risques en sécurité de l'information, recommandée par de nombreux référentiels comme la norme ISO 27001 est en train de devenir une obligation pour les responsables de la sécurité de l'information (RSSI), les directeurs des systèmes d'information

(DSI), et bien d'autres acteurs de l'entreprise. D'après l'AFAI (2008), La norme ISO 27001 définit la Politique du Management de la Sécurité des SI au sein d'une entreprise.

L'avènement de la norme ISO 27001 qui permet d'organiser sereinement sa sécurité des systèmes d'information sous forme d'un système de management de la sécurité de l'information (SMSI), impose une approche par la gestion des risques.

La norme ISO 27005 est un guide définissant une méthode d'appréciation des risques en sécurité de l'information. L'ISO 27005 a fait l'objet d'un consensus international et elle permet une meilleure compréhension mutuelle à travers le monde. L'ISO 27005 apporte une nouveauté fondamentale par rapports aux méthodes qui l'ont précédée comme EBIOS ou Mehari : la gestion des risques dans la durée, dans le temps. Il ne s'agit plus de gérer les risques en y travaillant dur quelques semaines, puis en recommençant son travail quelques années plus tard, mais de gérer les risques en sécurité de l'information au quotidien. Ce changement majeur est imposé par l'approche continue de l'ISO 27001, mais il représente le principal changement par rapport aux méthodes antérieures.

L'ISO 27005 est également la première méthode qui impose à la direction générale d'être parfaitement informée, et lui impose de prendre ses responsabilités en toute connaissance de cause, ce qui clarifie les responsabilités et facilite les arbitrages budgétaires.

2.4. Propositions de stratégies globales pour l'amélioration de la sécurité informatique

Pour être efficace, la politique de sécurité informatique de l'entreprise se décide à partir de fondements théoriques qui vont déterminer l'application de règles dans toute l'entreprise. On peut diviser le dispositif de stratégies sécuritaires à mettre en place en quatre volets qui se complètent : La prévention pour éviter les dommages (A), la défense proprement dite (B), le contrôle des moyens mis en place (C) et la réaction (D)

2.4.1. La prévention

La prévention s'exprime d'une part par une politique de cloisonnement des informations, et d'autre part par des règles de comportement des utilisateurs du système informatique.

2.4.1.1. Le cloisonnement de l'information

De nombreuses organisations, dont les entreprises et particulièrement les plus grandes d'entre elles appliquent une politique de cloisonnement de l'information. Ce système entraîne une difficulté accrue d'accès aux informations importantes car une intrusion dans un compte donné ne peut donner accès qu'aux informations nécessaires au travail du possesseur de ce compte et donc limite l'étendue des dégâts.

De plus, les informations sont classifiées selon leur confidentialité, les informations « normales » n'étant pas pour autant publiques. Les informations classées « confidentielles » (par leur auteur) obéissent à des règles strictes garantissant leur non-circulation à l'extérieur de l'entreprise et une circulation limitée à l'intérieur de l'entreprise.

Ce principe est à la base de règles de comportement des employés vis à vis de l'information et des systèmes informatiques.

2.4.1.2. Des règles comportementales

Dans le but de garantir la sécurité des informations, des règles régissant le comportement des employés doivent être mises en place.

Par exemple, chaque employé a son compte d'accès rigoureusement personnel au système informatique. De plus, il doit protéger son matériel par au moins un mot de passe s'il quitte son bureau. Le mot de passe lui-même doit être choisi en fonction de règles visant à limiter le hacking par des techniques dites de force brute (un programme qui essaye tous les mots d'un dictionnaire et d'autres combinaisons). C'est pourquoi, notamment, il doit contenir au moins un caractère numérique et un caractère alphabétique, tout en comprenant au moins six caractères sans comprendre deux caractères identiques consécutifs, et doit être changé tous les six mois.

Dans le même ordre d'idée, on peut aussi citer la règle du « bureau vide » selon laquelle un employé doit laisser son bureau vide de tout document lorsqu'il quitte son lieu de travail, de manière à limiter les risques d'espionnage. Aussi, les possesseurs d'ordinateurs portables sont tenus d'interdire l'accès à leur machine à toute personne qui ne travaille pas à l'intérieur de l'entreprise, au moyen de plusieurs mots de passe (au lancement de la machine ainsi que sur l'écran de veille).

Tous ces moyens de préventions sont bien évidemment essentiels à la protection du système informatique. Mais des moyens de défense plus techniques sont tout de même nécessaires.

2.4.2. La défense

La défense passe d'abord par une surveillance du système d'information, de manière à détecter le plus rapidement possible une intrusion, qui se heurtera à des moyens techniques de protection. Mais il faut tout de même prévoir une issue de secours, en cas de problème important.

2.4.2.1. La surveillance du réseau

Toute l'activité d'un réseau peut être surveillée à chaque instant grâce à des solutions matérielles ou logicielles spécialisées. Le flot de données généré par ces outils est bien sûr très important, mais il est possible de filtrer celui-ci de manière à obtenir les informations qui pourraient révéler une pénétration du système. De même, ces données peuvent être enregistrées pour être ensuite analysées sur la durée. On peut, par exemple, enregistrer toute l'activité d'un employé de la société pendant une période définie.

Un tel outil est bien sûr, très intéressant dans une optique de défense contre une attaque informatique, car il permet d'une part de détecter une intrusion extérieure, mais il permet aussi d'observer des employés susceptibles de perpétuer une telle attaque de l'intérieur.

Mais ces procédés se heurtent dans certains pays à la protection de la vie privée, et plus spécialement à la loi informatique et liberté.

Par contre dans des pays comme les Etats Unis ou l'Angleterre, ces méthodes sont tout à fait légales.

Mais, ce n'est pas tout de surveiller son réseau, il faut aussi prévoir des moyens interdisant toute intrusion extérieure.

2.4.2.2. La défense statique

La défense du réseau contre les attaques extérieures est assurée tout d'abord par son architecture. Celle-ci vise à limiter les points d'interconnexion entre le réseau interne et internet. A ces points sont placés des gardes barrières (aussi appelé firewall qui peut être aussi

bien un logiciel installé sur un routeur qu'un matériel spécifique) dont la fonction est de filtrer les données reçues ou envoyées.

Il peut prendre place sur une machine dite « système bastion » qui assure des fonctions de passerelle applicative (proxy), d'authentification des flux entrants, ainsi que d'audit, traçage ou logging des flux. Un firewall peut aussi être intégré à un routeur, qui assure ainsi des fonctions de filtrage.

Un niveau de sécurité supplémentaire peut être assuré en ayant recours à des techniques de cryptographie. Selon Louis Granboulan (2003 : 73) « la cryptographie est une composante essentielle de la sécurité des systèmes d'information. C'est la science qui étudie les méthodes (mathématiques) permettant d'obtenir confidentialité, intégrité et authenticité ».

2.4.2.3. Le plan de continuation de l'activité

Une attaque couronnée de succès, ou tout simplement une erreur humaine peut entraîner une paralysie ou une altération du système d'information. C'est pourquoi les grandes entreprises disposent d'un plan de continuation de l'activité.

Concrètement, ce plan est représenté par un ensemble de procédures d'urgence ainsi que par un enregistrement des données du serveur sur un site miroir, ce qui permet en cas de problème à un instant t, de récupérer les données de l'instant t-1. Ce site est de plus situé à un endroit tenu secret. En cas d'alerte, certains employés doivent s'y rendre de manière à pouvoir assurer la continuité de l'entreprise.

Toutes ces procédures et techniques misent en œuvre doivent bien sûr être contrôlées et testées.

2.4.3. Le contrôle

- ✓ le contrôle doit être assuré par des procédures d'audit ;
- ✓ la défense mise en place est ensuite testée.

2.4.3.1. L'audit de sécurité.

L'audit de sécurité s'entend tout d'abord comme une évaluation des procédures mises en place pour assurer la sécurité du système. Il va être effectué à l'aide d'outils informatiques

permettant de détecter les failles du système en générant automatiquement des tentatives de pénétration selon diverses méthodes préprogrammées et reprenant en général les techniques utilisées par les hackers.

2.4.3.2. Une équipe de hackers

La plupart des pirates informatiques trouvent aisément du travail lorsque l'envie ou le besoin de se reconvertir se fait sentir ainsi parmi les employés de la société il serait intéressant d'avoir une équipe de hackers chargée de tester la solidité des défenses de son système. Il agissent d'une manière indépendante et sont un moyen efficace pour améliorer la sécurité du système parce que d'une part, ils peuvent se montrer inventifs en imaginant de nouvelles techniques (non comme un logiciel), et d'autre part, sont probablement informés des techniques inventées par leurs collègues hackers du monde entier.

2.4.4. La réaction

S'il est important de savoir qu'une attaque est en cours ou qu'une attaque a réussi il est encore plus important de se donner les moyens de réagir à cet état de fait. C'est l'aspect le plus négligé actuellement même au sein des acteurs majeurs de la sécurité informatique. Pourtant, il n'est pas possible d'oublier les credo de tous les consultants en analyse de risque : " le risque zéro n'existe pas " ou encore " il n'y a pas de sécurité absolue ". Il faudrait donc toujours prévoir et se préparer au pire. Cela implique la mise en œuvre de procédures d'exploitation spécifiques à la réaction en cas d'attaque, la rédaction et le test d'un plan de continuité informatique à utiliser en cas de sinistre grave. Il est également primordial de se doter des outils permettant d'une part de collecter toutes les informations pouvant être nécessaires en cas de recours juridique. Un cadre doit aussi être prévu au niveau des responsabilités ; de ce fait les contrats d'assurance devront prendre en compte le risque représenté par les pirates. Le marché couvre très mal cet aspect à l'heure actuelle. Il n'existe que très peu de sociétés proposant une offre réelle en investigation d'incidents. Par ailleurs, même si certains cabinets de juristes se spécialisent dans le droit de l'Internet, la couverture du risque informatique et la définition des " éléments de preuve " dans les affaires de crimes informatiques restent encore floues.

Conclusion

La prise en compte des problématiques de sécurité est en cours actuellement dans une vaste majorité d'entreprises mais pour l'heure les moyens mis en œuvre ne sont pas toujours suffisants. Afin de supporter les entreprises dans leur processus de sécurisation, le marché, en forte croissance, s'est d'abord structuré dans le domaine de la Prévention. Néanmoins, de très nombreuses questions restent encore sans réponse dès lors qu'il s'agit de Détection et de Réaction. Ces deux domaines qui touchent à l'exploitation au quotidien (ou encore opération) des infrastructures de sécurité sont encore pleins de promesses mais aussi sources d'inquiétude pour les différents acteurs de la sécurité informatique.

Chapitre 3 : METHODOLOGIE DE L'ETUDE

Les chapitres précédents nous ont permis de présenter la sécurité informatique ainsi que l'assurance qualité de celui-ci. Nous passerons ainsi à la présentation de notre modèle d'analyse qui nous permettra de mener à bien la partie pratique de cette étude. L'élaboration d'une démarche référentielle d'assurance qualité de la sécurité du système informatique est l'objet de ce chapitre; pour ce faire, le travail sera réparti en deux parties. La première consistera à la présentation de notre cadre de recherche et à la recherche documentaire, la seconde mentionnera les outils de collecte et d'analyse des données.

3.1. Cadre de recherche

Le choix d'une méthodologie de recherche n'est pas fortuit, elle dépend des concepts utilisés et des objectifs fixés. En effet, on se base sur une approche et un type de recherche en adéquation avec son étude. Ainsi, le développement qui suit mettra en évidence le choix d'une approche et d'un type de recherche.

3.1.1. Le choix d'une approche

Il existe deux approches : l'approche inductive et l'approche déductive.

L'approche inductive se base sur des observations limitées et à partir de ces observations on inférera des hypothèses et des théories. Elle constitue une base importante du processus de recherche, surtout lorsqu'on est dans un domaine non étudié. Il s'agit d'une démarche qui est donc courante lorsque l'on est dans une étude ou une phase exploratoire. L'approche inductive constitue d'ailleurs souvent une phase initiale pour aider à formaliser des hypothèses dans le cadre d'un processus qui sera ensuite déductif.

L'approche déductive, quant à elle, consiste, à partir des connaissances, théories et concepts, et à émettre des hypothèses qui seront ensuite testées à l'épreuve des faits. C'est ce processus qui est appelé démarche hypothético-déductive. Cette démarche consiste à partir de la littérature existante à émettre des hypothèses qui seront testés sur un échantillon représentatif. Pour notre travail, nous avons opté pour cette dernière démarche car, elle permet de vérifier les hypothèses déduites.

Après le choix de l'approche, il paraît important de présenter les différents types de recherches.

3.1.2. La recherche documentaire

L'assurance qualité des sociétés n'étant pas monnaie courante au Sénégal, la recherche documentaire a constitué le fondement du présent mémoire. Des ouvrages, des articles, des rapports de recherche, des sites internet et des documents divers ayant trait aux systèmes informatiques et aux techniques d'assurance qualité informatique ont été consultés pour l'élaboration de ce travail. La lecture issue de cette recherche a servi à s'informer des recherches déjà menées sur le thème du mémoire et à situer la nouvelle contribution envisagée par rapport à elles. Il sera en outre possible de mettre en évidence la perspective qui paraît la plus pertinente pour aborder l'objet de recherche.

Il s'agit ici de préciser le cadre de notre recherche dans lequel nous choisirons une approche et le type de recherche et de définir la méthode de collecte des données après avoir décrit notre échantillon.

3.2. Les outils de collecte

Cette étape est celle qui nous a conduits sur le terrain afin de collecter les informations relatives à notre étude. Il s'agit pour nous ici de présenter l'outil de collecte des données et son contenu, de codifier le questionnaire et de préciser la méthode d'administration du questionnaire.

3.2.1. Les interviews

D'autre part, pour comprendre la politique du système de sécurité informatique existant au sein de Star Oil, des interviews ont été menées auprès des responsables de la société. En outre, pour avoir eut une idée sur le système informatique existant d'autres interviews ont été menées auprès du prestataire informatique de la société.

Ces interviews ont été réalisées sur la base d'un formulaire de questionnaires basé sur un guide d'entretien du logiciel Auditsoft et adapté à la réalité de Star Oil. Les informations qui y ont été tirées n'ont pas été exhaustives, mais ont permis de compléter les connaissances tirées des ouvrages, articles, rapports et site Web consultés à propos et de prendre conscience de quelques aspects de la question. Ces entretiens exploratoires complètent concrètement les lectures, ils nous ont permis de prendre conscience des différents aspects de la question, absents de notre propre expérience et de nos lectures.

Le guide d'entretien a été réalisé dans un premier temps en définissant cinq groupes de questions devant permettre de tester les cinq hypothèses, plus un groupe de questions introductives d'ordre général. Cet ensemble de questions a ensuite été soumis à un premier entretien (préparatoire) ayant permis de reformuler les questions dans un ordre logique, fluide, allant des notions les plus générales aux plus précises. Certains entretiens ont tous été enregistrés afin d'être retranscrits et analysés. Ceci nous a permis une analyse déductive, c'est-à-dire en regroupant les questions en fonction des hypothèses initiales auxquelles elles se rapportent afin de les confronter aux résultats.

En pratique, le contenu des retranscriptions a été réparti en vue de son interprétation en six fichiers correspondant aux cinq hypothèses et au contexte général.

Enfin, les réponses ont été rassemblées dans un tableau afin d'observer les tendances en fonction des dimensions analysées.

Les contraintes pratiques notées au niveau de la société Star Oil nous ont amené à faire preuve d'une certaine souplesse dans notre approche :

- ✓ tout d'abord, la durée des interviews a été ramenée à une heure au lieu deux heures entière initialement prévue.
- ✓ ensuite, certaines interviews ont été réalisées en groupe.
- ✓ de plus certaines personnes n'ont pas pu être interviewées faute de temps ou de disponibilité.
- ✓ enfin, pour l'entreprise ayant fermé ses portes, les questions ont été envoyées par email et n'ont pas fait l'objet d'une interview en face-à-face.

Au final nous avons eu l'occasion d'interviewer la majorité du personnel, ceci nous a permis de comparer la maturité et la qualité de leur politique de sécurité informatique. Cela nous a fourni des informations très enrichissantes qui nous serviront dans la conclusion de ce travail.

Cependant, nous avons fait face à quelques difficultés liées au refus de certains enquêtés de répondre à nos questions et au non respect de rendez-vous.

S'agissant de la première difficulté de l'enquête, enquêtés refuse catégoriquement de répondre à nos questions. Malgré les explications qu'on leur donnait, ils ne voulaient même pas voir le

questionnaire. Nous comprenons que ce genre de personnes ne sont pas instruits et ne sont pas habitués aux recherches.

La deuxième difficulté est le non respect de rendez-vous pour ceux qui ne répondent pas directement aux questions. A plusieurs reprises les enquêtés n'honorent pas au rendez-vous qu'ils avaient donné eux-mêmes sous prétexte qu'ils sont occupés. C'est pourquoi la plupart de ces questionnaires ne sont pas recouvrés.

Ainsi la technique de collecte des données étant présentée, il convient maintenant de passer aux outils qui nous permettront d'analyser nos données collectées.

3.2.2. Le questionnaire

Par définition, le questionnaire est un instrument de collecte des données, caractérisé par un document écrit, standardisé, comportant une série de questions écrites, adressées aux sujets concernés par la recherche en cours. Le questionnaire se fait avec des questions ouvertes plus quelques questions préformées.

Les questions prescrites sont retenues par les indicateurs caractérisant les différents concepts constituant le cadre théorique opérationnalisé. Les questionnaires ont pour objectifs d'obtenir des informations précises sur un thème particulier, comparer des informations, décrire une population et de vérifier une hypothèse en traduisant les objectifs de la recherche en question permettant de la confirmer ou de l'infirmer. C'est donc ce document qui nous a permis de collecter les données auprès de l'entreprise. Vu l'importance de cet instrument qui permet un contact entre les chercheurs et les répondants, son élaboration doit faciliter ce contact. Ainsi, il s'agit de commencer le questionnaire en posant des questions générales relativement neutre et facile et centrer progressivement l'interrogation sur des questions plus précises et plus difficiles. Dans le cas de notre étude qui porte sur l'assurance qualité de la politique du système informatique, nous avons commencé nos questions par celles relatives à la sécurité du système, suivi de celles liées l'assurance qualité de celle-ci et nous avons fini par celles axées sur l'identification des risques liés. La plupart de nos questions sont des questions fermées. Pour ces dernières, le répondant a le choix entre plusieurs modalités de réponse. Certaines de nos questions sont ouvertes, lesquelles des questions dont les modalités de réponse ne sont pas données. L'enquêté peut répondre librement à ces dernières. Maintenant, il paraît important de voir le contenu de notre questionnaire.

3.2.3. L'observation physique

Selon RENARD (2010 : 137), « l'observation physique est un outil d'application universelle. On peut observer les processus, les biens, les documents ou les comportements. L'observation peut être directe (réalisé par l'auditeur) et conduire à un constat ou indirecte (c'est-à-dire réalisé par une tierce personne) ». Il permet de s'assurer de la réalité, de la permanence ou de la conformité des dispositifs en place.

3.3. Outils d'analyse des données

Les données collectées sur le terrain doivent être soumises aux tests appropriés et les résultats qui en découleront vont servir à confirmer ou à infirmer nos hypothèses de recherche. Nous allons donc définir ici les différents tests statistiques qui vont nous servir d'analyser ces données. Il s'agit entre autres le tri à plat, l'analyse par correspondance principale. Nous développons successivement ici ces différentes méthodes qui ont permis d'analyser nos données. Il s'agit du tri à plat et de l'analyse des risques.

3.3.1. Le tri à plat

Le tri à plat est un test qui permet de contrôler la qualité des données collectées, de connaître le nombre de répondants pour chaque modalité de réponse (variable), puis en indiquant le pourcentage des répondants (fréquence relative). On peut ainsi détecter les erreurs de codification, des erreurs de saisie ou des erreurs de transcription des codes du questionnaire grâce au tri à plat.

3.3.2. Le tableau des risques

Il sert à l'identification des risques. Ce tableau découpe l'activité (la fonction ou le processus) objet de l'audit en tâches élémentaires. Il permet d'associer à chaque tâche, les risques susceptibles de se produire si son objectif n'est pas réalisé et les pratiques d'organisation admises ou dispositif de contrôle interne. En fonction du degré d'affinement de l'analyse, il comportera de 3 à 8 colonnes. C'est à partir de ce tableau que l'auditeur interne précisera les objectifs de sa mission.

Conclusion

La revue de la littérature a permis de présenter le système informatique ainsi que l'assurance qualité de la sécurité du système et notre démarche référentielle. L'inhérence des risques informatiques nécessite de leurs accorder une attention particulière. Les entreprises qui évoluent dans le secteur énergétique sont concernées par cette assertion. Le système informatique de la Star oil est particulièrement concerné par ces risques.

Conclusion de la première partie

Les mutations technologiques en cours posent des exigences de performance. Cela passe par la connaissance du niveau de sécurité actuelle notamment celle du système informatique. Le support le plus adéquat à cette mesure est de procéder à l'assurance qualité de la politique de sécurité du système informatique car, il attirera l'attention des dirigeants et des autres membres de l'organisation sur le niveau de sécurité et les menaces qui pèsent sur la performance de l'entreprise et permettra de définir des axes d'amélioration de ce processus hautement stratégique.

DEUXIEME PARTIE :

CADRE PRATIQUE DE L'ETUDE

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs. Cela a pour conséquence de les exposer à de nouveaux risques pour leurs activités, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser, le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

La sécurité informatique nécessite donc une véritable prise de conscience et la mise en place de mesures techniques et organisationnelles adéquates.

L'activité à laquelle s'adonne la Star Oil qui est la vente de produits pétroliers, est l'objet d'importants risques. Il convient donc d'effectuer une assurance qualité de la sécurité du système informatique. Elle constituera donc l'objet de cette seconde partie.

Nous présenterons dans cette deuxième partie la Représentation de la société Star Oil et les services impliqués dans le processus de sécurité du système informatique, nous ferons ensuite une présentation des points forts et points faibles du système informatique et nous achèverons cette partie par des recommandations à l'entité étudiée.

Chapitre 4 : PRESENTATION DE LA SOCIETE ENERGETIQUE STAR OIL

Cette section, consacré à la star oil, se préoccupera essentiellement de la présentation de la société, en donnant et épinglant des éléments susceptibles de fournir une quelconque information ou susceptibles de donner une idée sur ce qu'est la star oil pour nous permettre de nous fixer sur la gouvernance, les activités,... de notre champs d'investigation. Nous allons ainsi faire une brève présentation de la star oil, son évolution et stratégie ainsi que son plan d'organisation et système de gestion.

4.1. Brève présentation de Star Oil

Star Oil est une société anonyme au capital de F.CFA 200 000 000, spécialisée dans la commercialisation et la distribution de produits pétroliers et dérivés, et qui a été créée le 31 juillet 2003. Elle est située sise au quartier Ouest Foire, Cité Air Afrique n° B47 Dakar.

Depuis sa création la société s'est orientée dans la construction d'un réseau de points de vente, conforme à la réglementation en vigueur et aux standards généralement admis. Il s'agit à cet effet de stations service (terre), de stations de remplissage ou de stations dédiées à la pêche.

Par l'arrêté ministériel n°2180 MEM-CAB-CT.IB en date du 25 février 2004 « STAR OIL SA » est autorisée à exercer une activité de distribution d'hydrocarbures raffinés pour une durée de dix ans renouvelable.

C'est ainsi qu'elle a pour objet tant au Sénégal qu'à l'étranger :

- ✓ La recherche, l'achat, le traitement, le chargement , le transport et la distribution de tous produits pétroliers et dérivés notamment tous carburants, hydrocarbures et lubrifiants sous toutes ses formes ;
- ✓ L'importation, l'exportation, la commercialisation, le raffinage et le stockage de ses produits ;
- ✓ La création, l'acquisition et l'exploitation de toutes unités industrielles et de tous établissements, fabriques, magasins, entrepôts et dépôts de ces produits ;
- ✓ Et d'une manière générale, toutes opérations commerciales, industrielles, mobilières et immobilières qui pourraient se rattacher directement ou indirectement à l'objet social

ou à tous autres objets similaires ou connexes, susceptibles d'en faciliter le développement, la réalisation ou l'extension.

4.2. Evolution et stratégie

Depuis sa création en Juillet 2003, Star Oil s'est orientée dans la construction d'un réseau de points de vente, conforme à la réglementation en vigueur et aux standards généralement admis.

Il s'agit à cet effet de point de vente (station service, d'une station de remplissage ou d'une station pêche).

Star Oil dispose actuellement de 17 stations « terre » et de 13 pompes « pêche » exploitées sous la marque commerciale de « Star Energy » ; et à cela s'ajoutent quelques clients industries dont les plus importants sont Générale d'Entreprises, TOM, SOCAS, SOGEC, SAF, AREZKI, DHF, CGC …

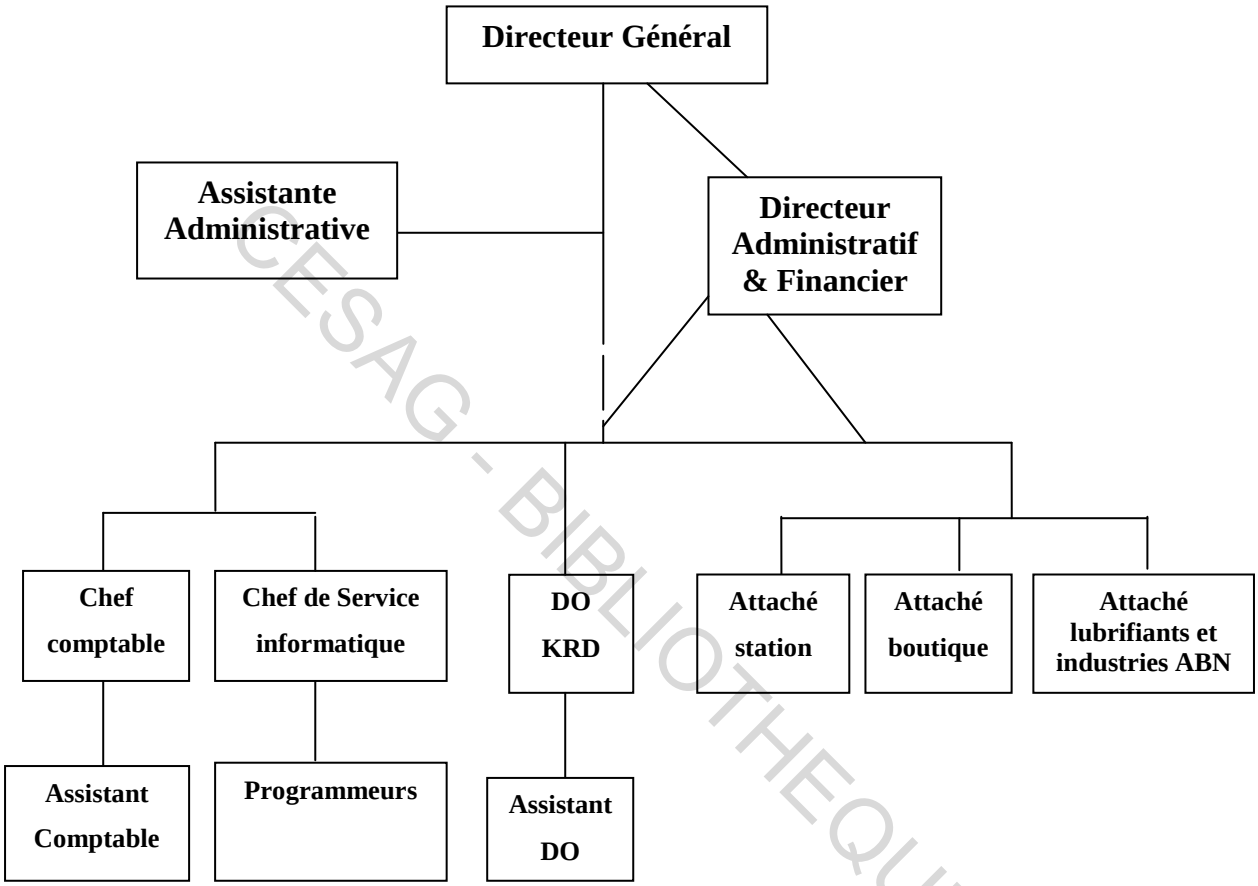
Elle compte dans son programme prévisionnel lancer cinq nouveaux sites entre Septembre 2009 et Septembre 2010 pour atteindre 20 à 23% de parts de marché.

Cependant Star Oil a pour principal fournisseur la SAR, Société Africaine de Raffinage qui possède des installations assez vieilles et mal entretenues. Par extension la continuité de l'exploitation de Star Oil est donc largement tributaire de la survie de la SAR si elle ne peut être en mesure d'importer sa consommation de produits raffinés.

4.3. Plan d'organisation et système de gestion

Le plan d'organisation de la Star Oil est défini par un organigramme. L'effectif permanent est de 23 salariés.

Figure 3 : Plan d'organisation et système de gestion



Source : Organigramme conçu à partir des informations de la direction générale

Conclusion

Nous avons effectué une présentation sommaire de la Star Oil, de son activité et des principaux éléments constitutifs du système informatique.

Cette présentation achevée, nous ferons une description du processus de sécurité et des services concourant à ce processus et nous présenterons le déroulement de nos travaux.

Chapitre 5: PRESENTATION DE LA POLITIQUE DE SECURITE INFORMATIQUE DE LA STAR OIL

Nous allons définir les intervenants et le rôle du responsable de la sécurité informatique, puis une présentation sera faite suivant l'ordre des objectifs définis au début de notre étude des mesures de contrôle en place. Le même découpage sera retenu pour l'identification et l'évaluation des forces et des faiblesses de l'assurance qualité du système de sécurité informatique.

5.1. Tâches du chef de service informatique

Le service informatique est directement rattaché à la Direction Administrative et Financière avec un effectif de deux programmeurs. Dans le cadre de ses missions, le chef de service informatique s'exécute aux tâches ci après :

- ✓ veille à la nouvelle technologie, afin de mettre les équipements de la Star Oil en phase avec ceux existants dans les entreprises similaires, en conformité avec les technologies et supports informatiques de dernière génération ;
- ✓ gestion et sécurité du réseau ;
- ✓ sauvegarde des données du réseau à temps et en espace et supports sécurisés ;
- ✓ gestion du parc informatique ;
- ✓ installation du matériel informatique ;
- ✓ gestion du site web, mise à jour du portail internet.

En sus un contrat de maintenance informatique à été signé avec le prestataire informatique ABCISS CONSULTING dans le cadre d'une gestion préventive trimestrielle et curative des installations et équipements informatiques.

Nous n'avons pu obtenir de fiche de poste, ni d'organigramme cacheté. Les fiches de postes n'ont pas également été mises à notre disposition.

5.2. Gestion des installations informatiques

Parmi les logiciels de gestion du parc informatique dont dispose le service informatique on distingue :

- ✓ le Soft delivery qui sert à effectuer des installations de programmes ou de logiciels à distance à partir d'un poste fixe ;
- ✓ le Desktop manager qui fait l'inventaire de ce qui existe au service informatique en l'occurrence le parc informatique soft et hard (+100 postes) ;
- ✓ le Remont acces ; qui sert à prendre en main à distance une machine et à dépanner les utilisateurs.

Chacun de ses logiciels est relié à un serveur informatique. L'accès au serveur et au logiciel est sécurisé par des mots de passe qui sont changés tous les mois. Des sauvegardes sont effectuées toutes les 24h à l'aide de bandes magnétiques et écrasées tous les (15jours). Pour les autres serveurs les données sont écrasées toutes les 48h.

Le système d'exploitation utilisé par les 2 serveurs est l'UNIX.

Il existe dans toutes les agences un réseau filaire TCP-IP brassé point à point et centralisé dans une armoire de brassage. Entre les agences se définissent deux (2) types de liaison qui relient les agences aux sièges :

- ✓ des Boucles Locale Radio ;
- ✓ des LS (Lignes Spécialisées).

5.3. Aspects sécuritaires

Nous distinguons la sécurité du système d'exploitation et la sécurité physique :

5.3.1. Sécurité du système d'exploitation

Chaque utilisateur se connectant au système est doté d'un mot de passe d'une longueur de 6 positions alphanumériques. La sauvegarde concerne principalement les données de la comptabilité et de la gestion commerciale. L'opération de sauvegarde n'est pas automatisée, elle se fait de façon manuelle et de manière quotidienne. Ces sauvegardes quotidiennes sont compilées par la suite en sauvegardes hebdomadaires. Les supports de sauvegardes utilisés sont des CD de capacité de 8 Giga. L'action de sauvegarde consiste à récupérer en fin de journée toutes les données journalières à la copier ou graver sous CD. Chaque sauvegarde sur CD est copiée au niveau du serveur.

En sus de ces sauvegardes une troisième sauvegarde est effectuée dans un disque externe d'une capacité de 160 giga octets. Les CD physiques ainsi sauvegardés sont conservés dans une armoire ignifugée qui se verrouille à clé.

Pour parer à toute rupture ou césure, le service informatique a mis en place des onduleurs de capacité respectives de 5000, 1100 VA, lesquels gèrent les serveurs et qui ont une autonomie chacune de 3 heures.

En sus de ce dispositif, Star Oil dispose d'un groupe électrogène, gérant tout le complexe de l'entreprise et qui se déclenche de manière automatique au bout de 30 secondes après survenance d'une quelconque rupture dans la distribution du courant du secteur des réseaux de la Sénélec.

5.3.2. Sécurité physique

La salle des machines de même que le bureau du chef de service sont sécurisés par accès à clé que possède le responsable informatique.

Conclusion

Ce chapitre a permis de se faire une idée de la sécurité informatique de la Star Oil à travers la présentation des principaux intervenants du processus et la description des mesures de sécurité existantes, permettant ainsi d'avoir une bonne idée de l'état des lieux. Cette description achevée, nous allons présenter les résultats de nos travaux de diagnostic. C'est l'objet du prochain chapitre de notre étude.

Chapitre 6 : ASSURANCE QUALITE DE LA POLIQUE DE SECURITE INFORMATIQUE DE LA STAR OIL

Cette section va présenter les forces et les faiblesses des processus de notre assurance qualité de la politique de sécurité informatique de Star Oil.

6.1. Points forts de la sécurité informatique

Les principaux points forts de notre étude d'assurance qualité, concernent essentiellement :

6.1.1. Gestion des installations matérielles

- ✓ l'électricité est fournie en continue par la centrale électrique qui dispose d'une arrivée de deux lignes de moyenne tension, d'un groupe électrogène et de batteries d'appoint ;
- ✓ les câbles hors bâtiments sont enterrés ;
- ✓ les serveurs de la salle informatique sont entretenus directement par le fournisseur.

6.1.2. Sélection du site et agencement

La salle informatique est bien aménagée et rangée.

6.1.3. Mesures de sécurité physiques / Accès physique

- ✓ l'accès aux informations sur les agences est limité par des armoires fermées à clés ;
- ✓ la salle informatique n'est pas facilement identifiable de l'extérieur ;
- ✓ les câbles de la salle informatique et des bureaux sont protégés par des goulottes.

6.1.4. Protection contre les risques liés à l'environnement

- ✓ les salles sont situées en hauteur dans le bâtiment ;
- ✓ la salle informatique dispose d'un compresseur pour éliminer la poussière sur les équipements.

6.1.5. Gestion des identités / Gestion des comptes d'utilisateurs

L'accès aux applications professionnelles est protégé par un processus d'authentification avec nom d'utilisateur et mot de passe.

6.1.6. Prévention, détection, neutralisation des logiciels malveillants

- ✓ La Représentation dispose d'un antivirus avec licence commerciale et mise à jour chaque année pour tous les postes, valide jusqu'au 10 novembre 2014.

6.1.7. Sécurité des réseaux / Echange des données sensibles

- ✓ Le système informatique de la Représentation est compartimenté ;
- ✓ L'antivirus NORTON dispose d'un pare-feu intégré.

6.1.8. Sauvegarde et archivage des données

- ✓ Les données sur tous les serveurs sont sauvegardées tous les jours en deux copies, CD et disque dur externe ;
- ✓ Les sauvegardes du réseau local sont archivées au Siège.

6.2. Points faibles de la sécurité informatique

Les principaux points faibles de notre étude d'assurance qualité, concernent essentiellement :

6.2.1. Organigramme et contrôle hiérarchique

Il apparaît dans l'organisation que le service informatique est structurellement rattaché à la Direction Administrative et Financière, cette situation est en contradiction avec les objectifs sécuritaires assignés à ce service du fait du caractère ultrasensible des informations qu'il centralise et ne garantit pas l'indépendance totale du chef de service dans l'exercice de ses fonctions.

6.2.2. Gestion des installations matérielles

La salle informatique est exiguë et non aérée, les équipements et certaines installations informatiques sont déposés à même le sol, et regorge des matières inflammables ;

Nous avons été témoin, lors de nos travaux, à l'arrêt du système, à plusieurs reprises à cause d'une panne du système.

6.2.3. Gestion des équipements informatiques

- ✓ les équipements informatiques dont disposent Star Oil sont assez obsolètes ;

- ✓ la salle informatique est facilement accessible ;
- ✓ les équipements nomades ne sont pas inventoriés.

6.2.4. Plan informatique

Une charte de bonne utilisation du système d'information n'a pas été rédigée et diffusée ;

Cette situation ne contribue pas à la sécurisation des données de Star Oil car le personnel peut effectuer des opérations pouvant poser des problèmes de sécurité.

6.2.5. Suivi des interventions

Le service informatique n'effectue pas de rapports d'évaluation ou de suivi de l'ensemble des interventions effectuées au cours d'une période et d'en évaluer les mesures futures à prendre dans le cadre de l'amélioration de ses propres performances et au-delà assurer une meilleure qualité du service au sein des différentes structures de la Star Oil.

6.2.6. Gestion des procédures informatiques

Le service n'est pas doté d'un manuel de procédures du système informatique ;

Le service dispose d'un schéma directeur informatique mais ne dispose pas encore de plan de secours.

6.2.7. Sensibilisation des agents

Absence de chartes et de sensibilisation des salariés de l'entreprise sur le système informatique.

6.2.8. Gestion des identités / Gestion des comptes d'utilisateurs

Une fois attribuée, les mots de passe qui peuvent être alphanumérique ou non, ne sont pas constamment mis à jour pour garantir la sécurité des informations ;

Egalement la direction n'effectue pas de lettre d'information à l'attention du service informatique pour leur signifier la rupture de contrat de tel agent afin de procéder à la suppression de son mot de passe et de son compte. La connaissance de départs de personnel est le plus souvent de manière informelle.

6.2.9. Sécurité des réseaux / Echange des données sensibles

Selon le service informatique la liste des habilitations ne comporte que les profils et les numéros de postes correspondants.

6.2.10. Audit de la sécurité

Absence de mission d'audit du système informatique.

6.2.11. Sauvegarde et archivage des données

La sauvegarde n'est pas automatisée.

6.2.12. Surveillance des systèmes

La supervision du système est effectuée tous les 15 jours.

6.2.13. Prévention, détection, neutralisation des logiciels malveillants

Le serveur Web reste vulnérable, lié à la configuration du Reverse Proxy qui pourrait permettre l'accès au système depuis Internet.

Chapitre 7 : RECOMMANDATIONS A LA DIRECTION DE STAR OIL

A travers ce chapitre nous allons énumérer quelques recommandations pour une bonne politique de sécurité informatique.

7.1. Organigramme et contrôle hiérarchique

Nous recommandons la correction de cette incompatibilité en rattachant le Service Informatique sous la responsabilité directe et unique de la Direction Générale.

7.2. Le soutien de la direction

Nous recommandons un meilleur soutien et implication de la direction de Star Oil. En effet le directeur général doit être un vecteur central pour la démarche de l'assurance qualité, par sa motivation et par les moyens financiers qu'il allouera aux services responsables. Les efforts financiers consentis doivent être perçu comme un investissement à part entière. On retrouve d'ailleurs cet engagement de la direction en tête, dans les normes ISO 9000 : 2000.

7.3. Sensibilisation des agents

L'engagement de la direction est nécessaire, mais non suffisant. La démarche qualité se décline à tous les postes de l'entreprise. Une formation technique, économique et culturelle est nécessaire pour que chacun prenne conscience que la qualité, c'est d'abord son propre travail, qu'une erreur mineure sur son poste peut engendrer pour la suite du produit ou du service des conséquences graves et, à terme, donner une image déplorable de l'entreprise.

Nous recommandons pour cela, la rédaction de chartes et la sensibilisation des salariés de l'entreprise ;

Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires, chaque utilisateur devrait au minimum chaque année se voir rappeler :

- ✓ le fait que les informations traitées doivent être considérées comme sensibles ;
- ✓ le fait que la sécurité de ces informations repose, entre autres, sur l'exemplarité de leur comportement et le respect des règles élémentaires d'hygiène informatique (non contournement de la politique de sécurité, verrouillage systématique de la session lorsque l'utilisateur quitte sa position informatique, non-connexion d'équipements

personnels au réseau de l'entreprise, non-divulgation d'authentifiant à un tiers, signalement des événements suspects).

Mettre en place une chaîne d'alerte connue de tous les intervenants. Tous les utilisateurs doivent pouvoir s'adresser à un interlocuteur unique pour signaler tout incident et être incités à le faire.

Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés, commencer par les composants de base (système d'exploitation, site bureautique, navigateur et outils nécessaires à la navigation, tels que la machine virtuelle Java ou le lecteur Flash, visionneuses de document) puis compléter l'inventaire avec l'ensemble des autres composants logiciels et intégrez ces éléments à la cartographie.

7.4. Gestion des installations matérielles

Nous recommandons :

- ✓ l'aménagement d'une salle plus spacieuse ;
- ✓ le renouvellement des machines informatiques.

7.5. Gestion des équipements informatiques

Nous recommandons de contrôler l'accès aux locaux et sécurité physique, la sécurité du système de contrôle d'accès aux locaux est bien souvent critique pour la sécurité d'une entreprise. En effet, dès lors qu'un attaquant parvient à obtenir un accès au sein du réseau interne de l'entreprise, les mesures de sécurité péri-métriques mises en place deviennent inefficaces.

Utiliser impérativement des mécanismes de contrôle d'accès robustes : Ils doivent permettre de définir des profils d'utilisateurs (employé, prestataire, stagiaire, etc.). Gérer rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme. Les règles suivantes doivent être appliquées :

- ✓ récupérer systématiquement les clés ou les badges d'un employé à son départ définitif de l'entreprise ;
- ✓ changer fréquemment les codes de l'alarme de l'entreprise ;

- ✓ ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs (agents de ménage etc.), sauf s'il est possible de tracer ces accès et de les restreindre ;
- ✓ techniquement à des plages données.

Codifier les immobilisations informatiques, en particulier les postes et supports nomades :

En effet la perte ou le vol d'équipements (ou de supports) mobiles ou nomades peut être lourd de conséquences pour l'entreprise : en l'absence de chiffrement les données (patrimoine technologique de l'entreprise, base de données clients) seront en effet compromises, et ce même si le terminal est éteint ou que la session utilisateur est fermée. Il est donc important de chiffrer les données sensibles sur de tels équipements. Nous recommandons aussi le renouvellement des équipements informatiques.

7.6. Gestion des identités / Gestion des comptes d'utilisateurs

Nous recommandons l'authentification des mots de passe car ils constituent souvent le talon d'Achille des systèmes d'information.

Il faudra aussi mettre en place des moyens techniques permettant de faire respecter les règles relatives aux mots de passe, ces moyens permettant de faire respecter la politique de mots de passe pourront être :

- ✓ le blocage des comptes tous les 6 mois tant que le mot de passe n'a pas été changé ;
- ✓ la vérification que les mots de passe choisis ne sont pas trop faciles à retrouver ;
- ✓ la vérification que les anciens mots de passe ne facilitent pas la découverte des nouveaux.

Ne pas conserver les mots de passe sur les systèmes informatiques. Les mots de passe ou les éléments secrets stockés sur les machines des utilisateurs sont des éléments recherchés ou exploités en priorité par les attaquants.

Nous recommandons la mise en place d'un système d'habilitation des profils et regroupant les aspects ci après :

- ✓ profils, en indiquant le nom prénom de la personne ;
- ✓ l'ensemble des exécutions ou opérations existantes (visualiser, modifier, détruire etc.) dans le système (réseau, paie, compta, courrier) ;

- ✓ les permissions fonctionnelles par oui/non selon le cas.

Il faudrait aussi envisager de recourir à une accessibilité par reconnaissance visuelle ou digitale au niveau de la salle informatique pour améliorer la sécurité de la salle des machines.

Ne pas donner aux utilisateurs de privilèges d'administration et ne surtout pas faire d'exception pour les dirigeants de l'entreprise.

N'autoriser l'accès à distance au réseau professionnel, y compris pour l'administration, que depuis des postes professionnels mettant en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes.

Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour. Il est important de disposer de la liste :

- ✓ des utilisateurs qui disposent d'un compte administrateur sur le système d'information;
- ✓ des utilisateurs qui disposent d'un poste non administré par le service informatique et donc non géré selon la politique de sécurité générale de l'organisme ;
- ✓ des utilisateurs qui disposent de privilèges suffisants pour lire la messagerie des dirigeants de la société ou a fortiori de l'ensemble des utilisateurs.

Rédiger des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires…). Elles doivent décrire :

- ✓ la gestion (création / destruction) des comptes informatiques et l'attribution des droits associés à ses comptes sur le système d'information, y compris pour les partenaires et les prestataires externes ;
- ✓ la gestion du contrôle d'accès aux locaux ;
- ✓ la gestion du contrôle des habilitations.

7.7. Sauvegarde et archivage des données

Nous recommandons la mise en place d'un système automatisé des sauvegardes programmées à une heure précise en fin de soirée. En outre, le service informatique devrait mettre en place un registre de tenue et de suivi des sauvegardes qui comporteraient les mentions suivantes :

- ✓ la date, l'heure de début et de fin de la sauvegarde ;

- ✓ les observations effectuées lors de la sauvegarde ou difficultés de la machine ;
- ✓ les signatures de la personne ayant effectué la sauvegarde ;
- ✓ de même qu'une partie des contrôles des sauvegardes effectives.

Un tel outil pourrait attester de l'effectivité des sauvegardes et identifier l'origine et la nature de quelconque problème ayant affecté l'action de sauvegarde ceci à titre préventif.

7.8. Suivi des interventions

Nous recommandons la mise en place de rapports périodiques retraçant l'ensemble des interventions effectuées par le service informatique et de permettre ainsi à la Direction Générale d'avoir une meilleure lisibilité sur les indicateurs de performance qu'elle a défini.

Tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires à la Direction Générale.

Inventoriez les sources susceptibles de remonter des vulnérabilités sur les composants identifiés et de diffuser des mises à jour (site des éditeurs des logiciels considérés…).

7.9. Gestion des procédures informatiques

Il faudra aussi mettre en place une cartographie précise de l'installation informatique et la maintenir à jour, cette cartographie doit au minimum comprendre les éléments suivants :

- ✓ la liste des matériaux et logicielles utilisées ;
- ✓ l'architecture réseau sur laquelle sont identifiés les points névralgiques (connexions externes, serveur hébergeant des données ou des fonctions sensibles, etc.).

Définir une politique de mise à jour et l'appliquer strictement, cette politique devra comprendre :

- ✓ les éléments à mettre à jour ;
- ✓ les responsabilités des différents acteurs dans cette mise à jour ;
- ✓ les moyens de récupération et de qualification des mises à jour.

7.10. Sécurité des réseaux / Echange des données sensibles

Limiter le nombre d'accès Internet au strict nécessaire : Il convient de connaître précisément et de limiter le nombre d'accès Internet et les interconnexions avec des réseaux partenaires au strict nécessaire de manière à pouvoir plus facilement centraliser et homogénéiser la surveillance des échanges.

Interdire la connexion d'équipements personnels au système d'information de l'entreprise : Si le travail à distance est nécessaire, l'organisme doit fournir des moyens professionnels pour permettre de tels usages.

Mettre à niveau les logiciels : Chaque jour, des vulnérabilités sont mises en évidence dans de très nombreux logiciels largement utilisés. En règle générale, quelques heures seulement sont suffisantes pour que des codes malveillants exploitant ces vulnérabilités commencent à circuler sur Internet. Il est donc très important d'utiliser en priorité des technologies pérennes dont la maintenance est assurée, d'éviter les technologies trop innovantes ou non maîtrisées en interne.

Sécuriser les équipements terminaux, s'il y a encore quelques années, les attaquants ciblaient d'abord et en priorité les serveurs, l'attaque d'un poste client est aujourd'hui le moyen le plus simple pour un attaquant de rentrer sur un réseau. En effet, il n'est pas rare que les postes clients soient moins bien sécurisés et surtout moins supervisés que les serveurs.

Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique, désactiver les services inutiles et restreindre les privilèges des utilisateurs.

Éviter l'usage de technologies sans fil (Wifi). Si l'usage de ces technologies ne peut être évité, cloisonner le réseau d'accès Wifi du reste du système d'information. L'usage des technologies sans fil n'est pas conseillé (faibles garanties en matière de disponibilité, difficultés de définition d'une architecture d'accès sécurisée à faible coût, etc.). Si de telles technologies doivent être employées, la segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion depuis la voie radio à un périmètre déterminé.

7.11. Audit de la sécurité

Faire réaliser des audits de sécurité périodiques (au minimum tous les ans).

7.12. Surveillance des systèmes

Cette supervision doit respecter les principes suivants :

Définir concrètement les objectifs de la supervision des systèmes et des réseaux. Quels sont les événements que l'on souhaite détecter ? Dans la majeure partie des cas, les événements suivants doivent impérativement générer une alerte qui doit impérativement être traitée dans les 24 heures :

- ✓ connexion d'un utilisateur hors de ses horaires habituels de travail ;
- ✓ transfert massif de données vers l'extérieur de l'entreprise ;
- ✓ tentatives de connexions successives ou répétées sur un service.

Conclusion

Cette deuxième partie a été l'occasion de présenter la Star Oil, sa politique de sécurité informatique et les dispositifs mis en place. Les informations reçues et collectées ont permis la mise en œuvre de notre démarche référentielle et la conduite de l'assurance qualité de la sécurité du système informatique. Ceci permettra à la Star Oil de corriger certaines défaillances constatées sur le plan organisationnel et fonctionnel.

CONCLUSION GENERALE

L’assurance qualité des systèmes d'informations prend tout son sens dans un contexte tel que celui dans lequel nous avons travaillé. La connaissance des principes de base de la sécurité ainsi que la mise en place d'une bonne politique de sécurité contribue à instaurer de manière générale un système d’information sécurisé et fiable.

Dans ce mémoire, nous avons présenté nos travaux sur la mise au point d’un processus d’assurance qualité de la sécurité informatique. Après avoir étudié les notions de base de la sécurité informatique, il est aussi apparu que l'environnement du système était une composante particulièrement importante et qu'il était intéressant d'intégrer les dirigeants pour l'évaluation de la sécurité. Nous avons aussi choisi d'étudier le processus d'attaque par l'exploitation d'une vulnérabilité.

Une première étape de cette approche a donc été l'identification et la caractérisation des notions importantes qui interviennent dans ce processus. Cette étude a mis en évidence en outre les facteurs environnementaux ayant une influence importante sur l’implantation du processus sécuritaire.

Ainsi l’objectif de ce mémoire visait à proposer non seulement un encadrement « juridico technique » pour les dirigeants qui veulent s’assurer de la conformité de leur entreprise aux obligations légales en matière de données personnelles, mais aussi à fournir à ceux ci une étude simplifiée du domaine de l’assurance qualité de la sécurité informatique. Ce travail de recherche met l’accent sur l’importance de la protection des informations de l’entreprise et ensuite des processus pour mener à bien l’élaboration de la politique de sécurité informatique, il convient donc en tout premier lieu de constituer un comité réunissant les différents acteurs du système informatique.

Il convient de définir actuellement pour Star Oil les risques engendrés par la défaillance du système informatique. Il faut pour cela avoir une vision globale du problème et connaître globalement les techniques à utiliser. Il s’agira ensuite d’analyser correctement les vulnérabilités propres à chaque type de menaces du système, de définir le niveau de sécurité requis et enfin de mettre en place une politique de sécurité acceptable. Lors de cette étape il faut bien veiller à examiner le problème tant du coté de l’administrateur que de celui du simple utilisateur.

BIBLIOGRAPHIE

OUVRAGES

1. AFAI (2008), Guide d'Audit des Systèmes d'Information: Utilisation de Cobit, IT Govemance Institute, Paris, 269 pages.
2. CARPENTIER, Jean-François (2009), La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques, Editions ENI, Paris 277 pages.
3. Cedric Llorens et Denis Valois, (2010), Tableaux de bord de la sécurité réseaux, EDITEUR : Eyrolles, 561 pages.
4. CNUCED/OMC, Application des systèmes de gestion de la qualité ISO 9000, CCI, Genève, 1996, 160 pages.
5. Didier Hallépée (2009), Conduite et Maîtrise de la sécurité informatique - la méthode CMSI, Carrefour du Net, 161 pages.
6. DURET D. & PILLET M (2002), Qualité en production - De l'ISO 9000 à Six Sigma, 2ème édition, Editions d'Organisation, Paris, 354 pages.
7. Éric Léopold et Serge Lhoste (2007), La sécurité informatique, P.U.F. «Que sais-je?», 128 Pages.
8. GODART, Didier (2002), Sécurité informatique: risques, stratégies et solutions, Edipro, Paris, 334 pages.
9. HAMZAOUl, Mohamed (2005), Audit: gestion des risques d'entreprise et contrôle interne: normes ISA 200, 315, 330 et 500. Editions Village Mondial, Paris, 242 pages.
10. Laurent Bloch, et Christophe Wolfhugel (2009), Sécurité informatique – Principes et méthode, Eyrolles, 292 Pages.
11. Louis Granboulan (2003), Cryptologie : le projet NESSIE, Les Cahiers du numérique 3/2003 (Vol. 4), 244 pages.
12. Marshall McLuhan « The Medium is the Message » 1967.
13. Riguidel (2003), Vers une conceptualisation de la sécurité des réseaux hétérogènes, Les Cahiers du numérique, 244 pages.
14. NF EN ISO 9000 : (2000), Système de management de la qualité - Principes essentiels et vocabulaire, AFNOR, France, (3.1.1), 30 pages.
15. REIX, Robert (2005), Systèmes d'informations et management des organisations. Se édition, LIBRAIRIE VUIBERT, Paris, 486 pages.
16. RENARD, Jacques (2010), Théorie et pratique de l'audit interne, 7e édition, Editions d'Organisation, Paris, 470 pages.

17. KALONJI BILOLO, la Sécurité Informatique au Congo, 2010, Editions Universitaires européennes, SARBRÜCK, 64 pages.
18. VOLLE Michel (2004), Lexique du système d'information. Club des maîtres d'ouvrages des systèmes d'information & Michel VOLLE, Paris, 23 pages.

SITE INTERNET

1. EFFI Soft (2010), Glossaire, *effisoft-consulting.com.* [En ligne] [Citation: 18 Aout 2010.] http://www.effisoft-consulting.com/Pages/Glossaire/Glossaire.aspx.
2. EOX PARTNERS SAS (2009), Charte informatique et Politique de sécurité. *Eoxpartners.jr,* [En ligne] 2009. [Citation: Il aout 2010.] http://www.eoxpartners.fr/charte _informatique politique-sécurité-eoxpartners.php.
3. GUIDE-INFORMATIQUE (2010), Sécurité des informations, normes BS 7799, ISO 17799, ISO 27001, EBIOS, MEHARI. *www.guideinformatique.com.* [En ligne] [Citation: 2 Septembre 2010.], http://www.guideinformatique.com/fiche-securite des informations-441.htm
4. PILLOU, Jean-François (2010), Mise en place d'une politique de sécurité. *Linux Plus- Value.* [En ligne] [Citation: 15 aout 2010.], http://www.linuxplusvalue.be/mylpv.php?id=184.
5. « village global » selon l'expression de Marshall McLuhan. http://fr.wikipedia.org/wiki/Marshall_McLuhan
6. Ministère de la justice, Ottawa, p. 14, en ligne : http://canada.justice.gc.ca/fr/ps/ec/chap/ch01.doc