ISO 27001… Faut-il certifier la sécurité des SI ?

Dans le cadre des rencontres d'ADELI… autour d'un verre

Martine Otter

Une nouvelle rencontre s'est tenue le lundi 15 mai 2006, sur le thème de la sécurité. Elle était animée par Lionel Vodzislawsky et Gilles Trouessin, tous deux certifiés "lead-auditor-27001" par le BSI. La question posée de façon très synthétique était la suivante : faut-il ou non se lancer dans un audit pour une certification ISO 27001/ISO 27002 ? Dans quelles conditions et dans quel but ? Nous ne rappellerons pas ici le fonctionnement de nos rencontres, déjà exposé à propos des logiciels libres dans cette Lettre. Nous vous proposons donc un résumé de l'exposé de nos deux conférenciers.

Les conférenciers

Nos deux conférenciers ne se sont pas présentés et nous le ferons donc pour eux :

- Lionel Vodzislawsky, ancien de la DGA et du Ministère des Finances, a été en charge, notamment, de représenter la France dans les instances européennes durant toute la période d'élaboration de la Directive Européenne sur la « Signature électronique ». Lionel est depuis quelques années consultant en « audit et sécurité des systèmes d'information » et actuellement gérant de la société OPPIDA Sud spécialisée, entre autre, dans les Systèmes de Management de la Sécurité de l'Information (SMSI) et dans les évaluations-sécurité (ITSEC, ISO 15408, etc.) et les audits-sécurité (ISO 27001 et ISO 17799) pour permettre la certification de la sécurité du système d'information.

- Gilles Trouessin est Docteur des Universités sur la « Sûreté de Fonctionnement et la Sécurité Informatique ». Après plus de 8 ans passés en tant qu'ingénieur d'études-sécurité pour le compte de la CNAMTS, Gilles, avec près de 19 ans d'expérience en « Sécurités », est auditeur, consultant et expert en Sûreté-Sécurité-Intimité des Systèmes d'Information, en particulier sur la Sécurité des Systèmes d'Information de Santé (les S.I.S.) et, tout particulièrement, sur la Sécurité des Systèmes d'Information Hospitaliers (les S.I.H.). Il accompagne actuellement une dizaine d'établissements de soins dans la prise de conscience de l'urgente nécessité de se familiariser avec la pratique du Management de la Sécurité de leur(s) Système(s) d'Information Hospitalier(s).

Sécurité de l'information et management de la sécurité

Lionel nous fit un exposé très pédagogique des principes de la sécurité de l'information. Il nous rappela les trois grands critères applicables en la matière que sont :

- la disponibilité de l'information ;
- son intégrité ;
- sa confidentialité ;

auxquels s'ajoutent d'autres critères relatifs au système de preuve tels que l'authenticité, la non-répudiation ou l'auditabilité, d'une manière plus globale et générique.

Il nous indiqua qu'il ne fallait pas confondre la sécurité de l'information et la sécurité informatique. Firewall, mots de passe et antivirus ne sont d'aucun secours si les aspects humains ne sont pas pris en compte : le maillon humain est réputé le plus faible en matière de sécurité.

Il nous dit aussi que la sécurité parfaite est possible, à condition de disposer d'un budget infini… Un management de la sécurité de l'information est donc nécessaire, puisqu'il faut établir des priorités. Ce management repose sur l'analyse et la gestion des risques et doit permettre de protéger l'information de façon active, en identifiant les menaces et en mettant en place les mesures de protection adaptées.

La notion de Système de Management de la Sécurité de l'Information, ou SMSI, est ainsi apparue, sur un modèle identique à celui du Système de Management de la Qualité, ou SMQ, et a conduit, dans le domaine de la sécurité, au développement de normes reposant sur le principe d'amélioration permanente de la « roue de Deming », suivant une logique similaire à celle de la famille ISO 9000 en matière de qualité.

De la BS 7799 à l'ISO 27002

Les premiers, les Britanniques ont développé dès 1995 la norme BS 7799, qui est un recueil de bonnes pratiques, regroupant 133 mesures, visant 39 objectifs dans 11 domaines. Il s'agit d'une boîte à outil et, en aucune manière, d'un référentiel de certification. Cette norme a été reprise par l'ISO en 2000, sous le nom d'ISO/IEC 17799 et devra être rebaptisée ISO/IEC 27002 lors de sa prochaine révision en 2007. Elle indique des objectifs-clés de sécurité et des mesures (ou exigences) de sécurité à mettre en place, tout en restant au niveau du « quoi ? » et pas au niveau du « comment ? » qui est à inventer par

chacun dans son contexte technique, organisationnel et humain spécifique.

L'ISO 27001

L'ISO 27001 est venue, fin 2005, remplir la fonction de référentiel de certification en matière de sécurité de l'information. Elle joue donc un rôle identique à celui de l'ISO 9001 en matière de qualité, tout comme l'ISO/IEC 27002 jouera un rôle identique à celui de l'ISO 9004. Cette norme est actuellement en cours de traduction en français, sous la plume, d'ailleurs, et donc le contrôle de Lionel Vodzislawsky. Il faut noter que la traduction de ce type de document technique est très délicate et que la traduction française de l'ISO/IEC 17999 comporterait de nombreuses erreurs, la rendant quasi inutilisable[1] ! AFNOR ne la commercialise d'ailleurs pas en français, laissant cette responsabilité à l'ISO.

Retours d'expérience

Gilles et Lionel, tous deux experts de la sécurité de l'information dans le monde de la santé, nous indiquent que ce milieu est encore « à l'âge de pierre » en matière de SMSI : si les aspects techniques informatiques sont à peu près maîtrisés, ceux relatifs aux ressources humaines, à la sécurité physique ou aux aspects juridiques ou à l'auditabilité sont bien souvent ignorés.

La contrainte juridique (i.e. légale et réglementaire) est sans doute le levier le plus efficace pour motiver et faire avancer la sécurité dans ce domaine. La certification H.A.S. (de la Haute Autorité de Santé), qui a pris le relais de l'accréditation ANAES pour les établissements de santé, se réfère ainsi aux quatre propriétés fondatrices de sécurité de l'information : Disponibilité, Intégrité, Confidentialité, Auditabilité (le quadruplet : D.I.C.A.).

Intégration des besoins qualité et sécurité

Est-ce si facile d'intégrer qualité et sécurité ?
« La sécurité des uns ne serait-elle pas source de non-qualité pour les autres et réciproquement ? »
Nous savons que « Le système le plus sûr est celui qui ne communique pas, voire celui qui n'est jamais branché sur le secteur ». Il est clair que si les besoins en matière de sécurité sont analysés de façon indépendante, ils risquent de ne pas être cohérents avec les besoins globaux du Système d'Information. Pour que le SMSI et le SMQ s'intègrent de façon harmonieuse, une approche globale est nécessaire, sinon on se retrouve avec deux systèmes de management qui ne se parlent pas.

Gilles Trouessin souligna que les personnes les plus réceptives à cette approche globale sont les personnes de la qualité, qui perçoivent bien la similarité des deux systèmes de management.

Paulette Pierrard nous fit remarquer au passage que l'imbrication entre qualité et sécurité est déjà présente dans les normes relatives à la qualité du logiciel, puisque l'une des caractéristiques qualité du logiciel est, précisément, la sécurité.

Des situations diverses

La culture du risque est très inégale suivant les domaines métiers.
Une majorité d'hôpitaux n'ont pas de structure de base en matière de sécurité de l'information.
Les milieux bancaires ont, par opposition, une culture du risque très forte qui leur permet de prendre leurs responsabilités en connaissance de cause : par exemple de décider de chiffrer ou non les transactions cartes. Suivant le cas, le risque peut être accepté, transféré au client ou à une compagnie d'assurance, ou faire l'objet d'actions de réduction…
Dans le milieu hospitalier, il existe depuis toujours d'autres risques que le risque financier, le risque humain étant le premier. Une réflexion globale sur le risque n'existe pas encore dans ce milieu.
La notion de confidentialité doit être appréciée différemment suivant le domaine : les données confidentielles du monde bancaire ne portent que sur des éléments financiers, celles du monde de la santé portent sur la personne en général et sur son intimité la plus critique : son état de santé. Chacun sait qu'il existe des obligations fortes en matière de secret médical, mais qu'elles ne sont pas respectées : aucun médecin n'a jamais été convoqué devant le juge d'instruction pour non-respect du secret médical, si ce n'est devant le Conseil de l'Ordre ! La disponibilité de l'information (les données médicales du patient) est le premier souci médical.
Les législations sont souvent non applicables : il faut sauver la vie d'abord, c'est l'urgence qui prime.

Questions pour une certification

Périmètre de certification ?

Comment délimiter un périmètre de certification ? La certification du système de management de la sécurité dépasse largement la sphère informatique, puisqu'elle s'intéresse aussi bien aux autres formes d'information que sont les documents papier et l'information orale.
Peut-on dans ce contexte faire certifier uniquement le périmètre d'une DSI à l'intérieur de l'entreprise ?
Les réponses furent prudentes : on peut bien sûr restreindre le périmètre mais en lui assurant une certaine cohérence.

Les errements de l'ISO 9000 ont servi de leçon : il ne faut pas oublier qu'un libellé de certificat doit être suffisamment clair. Un périmètre tarabiscoté sera non

[1] *Lire sur ce sujet dans cette même Lettre la nuance importante entre « traduction » et « interprétation ».*

publiable et ne donnera confiance à personne. Il faut que le périmètre soit clairement délimité en matière de site géographique et de processus. Certaines exclusions, comme par exemple celles de la téléphonie sont impossibles à gérer.

L'auditeur doit s'assurer de la compréhension du personnel : « laisser traîner ses yeux et ses oreilles ».
L'excès inverse est tout aussi dangereux : Orange UK a ainsi fait certifier en une seule fois toute son activité (13000 personnes). Ceci est remarquable, mais, avec un peu de recul, jugé peu sérieux par les professionnels. Le maintien d'une telle certification sera probablement difficile voire utopique.

Objectif de la certification

L'objectif d'une certification serait-il uniquement de communiquer sur le certificat ? Lionel nous rappela que le principe général d'une certification est attaché à un périmètre. L'entreprise certifiée a obligation de montrer le certificat qui indique le périmètre. Le grand public, faute d'éducation suffisante en la matière, n'est pas toujours informé de cet aspect. Entre professionnels, par contre, on sait clairement à quoi cela correspond. Chacun peut s'assurer que le périmètre certifié correspond à son besoin.

L'obtention d'une certification limite le nombre d'audits seconde partie, mais dans certains cas un complément d'audit peut rester nécessaire, lorsque le certificat ne couvre qu'une partie des systèmes mis en œuvre.

Si la communication peut être une première motivation pour l'obtention d'une certification, il faut noter que la démarche conduit naturellement à une prise de conscience des risques par le management, y compris dans des cas où cet aspect n'était que secondaire à l'origine : un tel cas nous a été cité par l'un des participants, en toute confidentialité naturellement.

Certification dans l'infogérance

Une société de service peut-elle se faire certifier sur un périmètre qu'elle ne gère pas encore ?
Oui et non : l'infogérant se fait certifier sur une démarche de prise en compte de la sécurité, pas sur les affaires qu'il va traiter demain. Il se fait certifier pour son système, pas pour son service actuel. Dans le cas de sites supplémentaires infogérés, ceci peut toutefois entraîner une extension au moins géographique du périmètre.

Qui certifie ?

Aujourd'hui, en France, aucun organisme n'a encore été accrédité pour la délivrance de certificats ISO 27001. Des dossiers ont été déposés auprès du Cofrac et sont donc actuellement en cours d'instruction. Il s'agit d'organismes généralistes de certification internationaux présents en France, tels que BSI ou BVQI, ou de sociétés françaises spécialisées en matière de sécurité telles que LSTI (www.lsti.fr).

Qui est certifié ?

Du fait de l'absence de société accréditée en France, les premières certifications ont été délivrées par des organismes étrangers comme le BSI. La société NRG du groupe Ricoh, ainsi que Axalto (ex Gemplus), dans le domaine des cartes à puce, ont été certifiées par le BSI sur la base de la norme BS 7799.
Certaines entreprises ont été auditées et sont d'ores et déjà précertifiées par des organismes en attente d'accréditation. On peut citer dans ce cas NTT/Verio (www.verio.fr).

Quelle priorité entre Qualité et Sécurité ?

La question posée était la suivante : dans quel ordre faut-il aborder la certification ? Faut-il d'abord mettre en place un Système de Management de la Qualité, puis, ensuite seulement, un Système de Management de la sécurité ? Ou l'inverse ?

En fait, il n'y a pas de réponse toute faite à cette question, tout dépend du contexte : il n'y a pas de priorité, les deux normes sont construites sur un même modèle, celui de la roue de Deming ; quel que soit l'ordre dans lequel on les met en œuvre, un système de management va de toute façon faciliter la mise en place de l'autre système.

Peut-on mener les deux de front ?

Il existe des certifications combinées : Qualité, Environnement, Sécurité de l'information.
Ce type de certification globale très ambitieuse poserait des problèmes et serait en voie d'abandon. Les qualificatifs d'« ambitieux » et de « masochiste » ont été employés pour qualifier une telle approche globale. Une démarche plus progressive est recommandée par les conférenciers et les experts de la sécurité présents dans l'auditoire.

Impact sur le coût des assurances

La certification ISO/IEC 27001 va-t-elle permettre de négocier à la baisse le tarif des assurances ? Nous savons depuis longtemps que les assureurs refusent le risque. Peut-on espérer un lien plus direct entre le niveau de sécurité et le coût de l'assurance ?
Nos conférenciers nous laissèrent peu d'espoir dans ce domaine.
Historiquement, les méthodes d'évaluation de la sécurité, telles que Marion ou Melissa, tirent leur origine du monde de l'assurance. Elles s'apparentaient à des questionnaires d'audit et conditionnaient la dégressivité des primes : si vous appliquiez les

bonnes pratiques, l'assureur acceptait de réduire ses tarifs.

Face à l'accroissement de la complexité des systèmes, cette époque semble aujourd'hui révolue. Les évaluations servent plutôt à identifier les points faibles pour lesquels une couverture par une assurance reste indispensable.
Pour éclairer cette problématique de l'assurance, Gilles Trouessin resitua la sécurité de l'information dans le contexte plus large de la sûreté de fonctionnement des systèmes.

L'approche globale de la sûreté de fonctionnement des systèmes (ou « dependability », en anglais) s'intéresse à la fiabilité (ou « reliability »), à la maintenabilité (ou « maintainability »), à la sécurité-innocuité (ou « safety ») et à la sécurité-immunité de l'information (ou « security »). En matière de fiabilité et de maintenabilité, des raisonnements probabilistes peuvent être tenus : les primes d'assurance peuvent s'appuyer sur des modèles probabilistes de taux d'accident, sur des espérances de vie. En matière de sécurité, la composante accidentelle n'est plus la seule à prendre en compte. Les attaques intentionnelles deviennent prépondérantes, l'attaquant connaît parfaitement les failles des systèmes et le succès d'une attaque ne relève plus seulement du hasard. Même lorsque le niveau de sécurité est de 99%, la catastrophe arrive et produit ses effets à 100% !
Dans le milieu de la santé il ne faut pas oublier que la sécurité de l'information (« security ») passe naturellement après celle des personnes (« safety »).

Dernière question : combien ça coûte ?

Comme en matière de qualité, les coûts directs d'audit et de certification sont peu élevés. Ils ne représentent que quelques jours d'auditeurs (entre 5 et 10 jours). Les coûts importants correspondent aux tâches de préparation et de mise à niveau du système.
Combien pèse le budget de la sécurité par rapport au budget d'une DSI ? La réponse est classique : cela varie énormément suivant les secteurs. Les budgets ne dépassent pas 1% dans le secteur hospitalier. Côté Télécoms et banques, ils se situeraient plutôt entre 5 et 10%.
La fourchette se situe généralement entre 3 et 10%, à comparer au budget de la qualité, pour lequel le chiffre de 5% est souvent avancé.
Encore faut-il relativiser les chiffres annoncés suivant la façon dont les dépenses sont imputées à l'intérieur d'une entreprise : la licence d'un antivirus peut être imputée sur la sécurité ou au titre de la bureautique. La seconde solution, intégrant le coût de l'antivirus dans le coût global du poste de travail présente l'avantage d'en admettre le côté incontournable : tout système devrait prendre en compte sa propre problématique sécurité. La question « avec ou sans sécurité ? » ne devrait pas se poser, tout comme la question « avec ou sans qualité ? ». La bonne question est celle du niveau de sécurité à mettre en place, en fonction de l'analyse des risques et des besoins.
Dans l'idéal, le budget « sécurité » ne devrait regrouper que les coûts relatifs aux aspects transversaux. Ceci milite dans le sens d'une fonction RSSI (Responsable de la Sécurité du Système d'Information) qui se situerait plutôt hors DSI, rattaché à la Direction Générale, ce qui semble aujourd'hui être de plus en plus la tendance.

Conclusion

Je retiendrai de cette soirée très dense le message suivant : la sécurité de l'information, comme la qualité de l'information, ce n'est pas le métier des informaticiens ! Cela ne peut se mettre en place de façon efficace dans une entreprise que par une prise de conscience au plus haut niveau des risques et des besoins. En gros, beaucoup de chemin à parcourir, avec au passage beaucoup de travail, de pédagogie et de persuasion, pour les consultants et les organismes de formation.

Après les applaudissements d'usage, Geneviève Coullault clôtura la séance en annonçant la sortie prochaine du « Guide des certifications SI » chez Dunod. Plusieurs dispositifs de certification dans le domaine de la sécurité y sont présentés, tant en matière de certification de système de management que de certification de produit et de personnes. ▲

martine.otter@adeli.org