Systèmes d'Information et Management

Volume 16 | Issue 4 Article 6

2011

Revue de thèse: MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION - Mise en oeuvre, évaluation et pilotage de la sécurité de l'information dans les organisations? (par N. Dagorn)

Alain Cucchi

Université de La Réunion - IAE la Réunion, alain.cucchi@univ-reunion.fr

Nathalie Dagorn

« MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION - Mise en œuvre, évaluation et pilotage de la sécurité de l'information dans les organisations »

Thèse soutenue le 30 septembre 2011 à l'Université de Nancy 2, sous la direction du professeur Jacques Thévenot.

La thèse rédigée par Mme. Nathalie Dagorn est de type thèse sur travaux. Elle comporte un volume de 411 pages dont environ 152 pages d'annexes générales (dédiées notamment aux listes des figures et des tableaux ainsi qu'à deux essais en langue anglaise) et 40 de bibliographie (contenant plus de 450 références). Chaque chapitre contient également des annexes spécifiques aux éléments traités.

La thèse est construite en 5 parties : l'introduction, trois parties principales et une conclusion. L'introduction (26 p.), développe la question de recherche principale qui est énoncée ainsi :

« Comment manager la sécurité de l'information dans les organisations ?»

L'auteur s'inscrit dans une perspective interdisciplinaire en s'appuyant sur les sciences de gestion, l'informatique et l'économie de la sécurité. Il développe une vision en cycle du management de la sécurité de l'information autour du triptyque « engagement, évaluation et pilotage ». Cette approche structure le document, les parties deux, trois et quatre traitant des dimensions évoquées. Dans son cadre conceptuel, l'auteur étudie les travaux traitant des aspects de la sécurité dans le champ du management des SI. Il distingue essentiellement les travaux ayant une approche technique, ceux privilégiant une approche managériale et ceux associés à l'économie de la sécurité. Cette revue de littérature montre l'importance des travaux centrés sur les aspects stratégiques au détriment des niveaux tactiques et opérationnels d'une part et l'importance d'une approche globale de ces questions d'autre part. Puis l'auteur décrit le contexte empirique de sa recherche dans les sociétés financières au Luxembourg et résume succinctement les parties développées dans le corps du document.

Le chapitre 2 (38 pages) « Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information » tente de répondre à la question « Pourquoi les organisations s'engagent-elles dans la gouvernance de la sécurité de l'information et quelles sont leurs pratiques ? ». Il s'articule en 3 parties. La première s'appuie sur une revue de la littérature pour construire et administrer un questionnaire quantitatif sur la gouvernance de la sécurité de l'information (140 entreprises luxembourgeoises contactées, 120 réponses). Ce questionnaire traite essentiellement du niveau de connaissance de la gouvernance de la sécurité de l'information (GSI), des enjeux stratégiques associés, des conditions de mise en œuvre, de l'organisation et de la maturité des organisations dans ce domaine. Les résultats descriptifs sont présentés. La deuxième

partie présente la restitution des résultats auprès de 68 responsables de la sécurité de l'information. Lors de cette restitution, une conférence débat a permis de valider des propositions dans les domaines suivants : domaines stratégiques concernés par la GSI, les référentiels de pratique et les capacités organisationnelles mises en œuvre. Le lecteur trouvera plusieurs annexes décrivant les référentiels de gouvernance de la sécurité de l'information, le questionnaire et le guide d'entretien utilisés, les détails des conclusions et des recommandations associés à ces études.

Cette recherche a permis de mieux caractériser quatre déterminants potentiels dans le processus d'engagement des organisations dans la gouvernance de la sécurité des SI, de produire une description détaillée des pratiques de gouvernance des entreprises étudiées et d'identifier des supports nécessaires à l'organisation de cette gouvernance.

Le chapitre 3 (46 pages) s'intitule « Evaluation et prévision de la sécurité de l'information par la théorie stochastique des jeux ». Il tente de répondre à la question « Comment évaluer le niveau de sécurité de l'information au sein des organisations ? ». Dans ce but, l'auteur utilise dans une première partie les apports de modèles de recherche en sécurité de l'information (modèles managériaux, économiques et informatiques) pour construire un modèle stochastique. Les éléments du « jeu stochastique » sont décrits et des scénarios d'évaluation sont proposés. Le modèle proposé intègre les attaques intentionnelles et les défaillances accidentelles. L'objectif est d'identifier les meilleures stratégies de réponse entre l'administrateur du SI et l'attaquant en utilisant l'équilibre de Nash. Dans la deuxième partie, ce jeu est confronté à des projets empiriques pour en étudier la pertinence et la validité.

Le chapitre 4 (43 pages) a pour appellation « Mesure de la performance et pilotage de la sécurité de l'information dans un tableau de bord équilibré sécurité (TBES) ». Il traite de la question « Comment piloter la sécurité de l'information dans les organisations ? ». S'appuyant sur les travaux de Kaplan et Norton, l'auteur propose un tableau de bord équilibré sécurité (TBES) permettant de piloter la sécurité dans les organisations. Dans ce but, l'auteur s'appuie sur une modération Metaplan, une étude de cas longitudinale et une analyse expost de quinze projets de sécurité pour identifier un ensemble de mesures quantitatives et qualitatives à intégrer dans ce tableau de bord spécialisé. L'intérêt principal de cette approche est de conserver les quatre dimensions originelles du tableau de bord de Kaplan et Norton pour proposer un instrument de mesure, de communication et de pilotage de la sécurité de l'information. En annexe de ce chapitre, le lecteur trouvera un guide de modération pour la méthode Metaplan, la description des projets de sécurité étudiés, des rapports de sécurité et des recommandations pour la mise en œuvre d'un TBES.

La conclusion résume le contenu de la thèse en s'attachant à mettre en exergue les apports de ce travail (d'un point de vue managérial et pour la recherche), les limites et les perspectives de recherche.

Dans ce travail doctoral de Sciences de Gestion, le thème de la recherche portant sur le management de la sécurité de l'information a été apprécié. C'est un thème important pour les entreprises avec un contexte réglementaire en

constante évolution. L'auteur propose une synthèse des référentiels, normes et pratiques dans ce domaine. C'est un des points forts de ce travail. L'auteur s'est également attaché à proposer des réponses aux aspects opérationnels du management de la sécurité de l'information. En développant une approche par les tableaux de bord équilibrés de sécurité (TBES), il propose une démarche et des outils pour mieux piloter la sécurité de l'information dans les organisations.

par Alain CUCCHI