ÉTUDES

1. LE LIVRE BLANC SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DES ÉTABLISSEMENTS DE CRÉDIT

La Commission bancaire vient de publier un « Livre blanc » sur la sécurité des systèmes d'information des établissements de crédit. En outre, M. Butsch, secrétaire général de la Commission bancaire a envoyé directement à chaque président d'établissement une lettre individuelle jointe en annexe 1 p. 32) pour appeler l'attention de celui-ci sur les risques que l'absence ou la mauvaise sécurité des systèmes d'information étaient susceptibles de générer.

• L'objectif visé par cette démarche est d'ordre pédagogique. Il est d'abord de sensibiliser à ces risques et de responsabiliser les dirigeants des établissements de crédit. In fine, au regard de la loi, ce sont bien eux qui sont responsables. Mais le but est aussi de leur fournir une base de connaissance, de réflexion et de travail minimum, c'est-à-dire de leur permettre de poser les questions essentielles à leurs collaborateurs en charge de ces questions et - pour le cas où ceci ne serait pas déjà connu - d'avoir une idée relative du niveau de sécurité de leur maison, mesure du niveau d'inquiétude qu'ils doivent ou non manifester à l'égard de ce domaine qui, pour technique qu'il leur soit présenté, demeure de leur responsabilité.

Le Livre blanc n'oublie ni les « débutants », techniciens en charge de ces questions, puisque le champ couvert par l'ouvrage est assez vaste et que les références essentielles sont indiquées, ni même les « spécialistes » que les réflexions sur ces thèmes, recueillies auprès de nombre de leurs confrères, peuvent intéresser. Certes, il existe de nombreux ouvrages techniques beaucoup plus précis ou détaillés mais aucun, à notre connaissance, n'est suffisamment synthétique pour s'adresser à différents publics, ni ne formule clairement de conseils ou de recommandations qui font de ce livre blanc un guide des meilleures pratiques: « a best practice paper ». D'autant que ce sont sur ces bases que l'inspection envoyée sur place auprès des établissements par la Commission bancaire pourra être amenée, éventuellement, à estimer le niveau de sûreté des systèmes sous revue.

• La raison de cette démarche est la suivante. L'informatique constitue depuis longtemps un « vecteur » possible de risque en tant que facteur déclenchant ou point de passage et de transmission mais, au fur et à mesure que les autres risques sont mieux encadrés, parfois d'ailleurs par des normes réglementaires, il est devenu nécessaire pour la Commission bancaire de s'en préoccuper également. Le risque sur les systèmes d'information fait partie intégrante de la « constellation des risques - auxquels les établissements sont confrontés. Il doit donc être correctement surveillé et géré par les agents désignés et contrôlé par les dirigeants responsables. Ces derniers, qui assument les grands arbitrages et la responsabilité face à leurs actionnaires et aux autorités de tutelle, ne peuvent se désintéresser de ce « domaine technique ».

Dans le domaine des « risques techniques », le risque sur les systèmes d'information est l'un des plus importants car, pour reprendre la terminologie utilisée sur les marchés, il a une très haute « volatilité » et possède un impact potentiel croissant. Ceci tient à ce que les transferts entre agents financiers ou entre agents financiers et agents non financiers se sont accrus dans des proportions exponentielles, notamment du fait des activités de marché sur instruments dérivés, réalisées sur une base de plus en plus internationale, impliquant un emploi massif de l'informatique et des télécommunications. Cette évolution rapide dans un monde complexe et incertain augmente la probabilité de mise en oeuvre de scénarios décrits par la - théorie du chaos. Enfin, les pressions sur la rentabilité bancaire résultant du resserrement des marges bancaires ou de la nécessité d'accroître les provisions laissent craindre un intérêt moindre pour les projets sécuritaires. C'est pourquoi la Commission bancaire a souhaité jouer un rôle pédagogique afin de provoquer une prise de conscience des dirigeants.

• Le contenu du Livre blanc a déjà été résumé dans plusieurs publications *(6) ou articles et a notamment fait l'objet d'une synthèse jointe en annexe à la lettre adressée aux présidents des établissements de crédit (cf. p. 32). Il ne paraît donc pas nécessaire d'y revenir ici, d'autant qu'un sommaire détaillé figure en annexe 2.

Ce livre blanc a été bien accueilli par la profession; l'adoption d'une démarche « consensuelle » et pragmatique, la définition d'un « noyau dur» des bonnes pratiques observées et proposées comme « point d'ancrage » à la réflexion et aux développements propres des établissements ont favorisé des retombées internes qui vont et qui iront dans le sens d'une meilleure sûreté de la place.

Tôt ou tard, la pression des gros clients, celle des contreparties bancaires et le développement des techniques comme l'échange de données informatisées (EDI), mais aussi l'accroissement des dangers liés à l'ouverture et à l'internationalisation des réseaux imposeront une parfaite maîtrise du risque sur les systèmes d'information - et notamment de celui sur l'informatique.

On estime que les sinistres ou les pertes informatiques sont, en France, imputables dans 58 % des cas à la malveillance, dans 25 % aux accidents et dans 17 % aux erreurs *(7) : l'impression qui semble se dégager de cette

statistique est que les pertes sont dues au facteur humain d'abord, aux matériels parfois, aux logiciels un peu plus rarement.

Mais il s'agit là, si l'on peut dire, des pertes de premier degré telles qu'elles sont déclarées aux compagnies d'assurance. Si, au-delà de l'apparence, on examine attentivement les cas de pertes ou de fraudes ayant eu, dans le monde, de graves conséquences, on trouvera, souvent, que l'informatique y a eu une part - volontaire ou involontaire - non négligeable. D'une façon ou d'une autre, l'informatique constitue, en tant que condition permissive, un facteur de risques, et cela d'autant plus qu'elle donne une impression exagérée de sécurité. Elle autorise en particulier des transferts rapides et des calculs ou opérations de volume très important qui peuvent rester « masqués » grâce aux énormes capacités offertes aux employés par les micro-ordinateurs installés - aux connections aux réseaux parfois réalisées de façon « sauvage » - et, de ce fait, peu contrôlables. De plus, elle constitue un « voile opacifiant » entre les opérations, la comptabilité et la transmission d'informations de synthèse à la direction générale nécessaires à la constitution des tableaux de pilotage et de surveillance des dirigeants (EIS ou executive information systems). Enfin, elle favorise la « complexification » de systèmes empilés que de moins en moins de personnes sont capables de maîtriser complètement en raison de l'imbrication des techniques et donc des techniciens. La fiabilité de ces systèmes, l'intégrité des données et la piste d'audit deviennent plus difficiles à garantir au moment même où ces instruments de pilotage apparaissent indispensables en raison de l'accroissement de la vitesse de réaction exigé aujourd'hui par les brusques mouvements de la conjoncture financière et le développement des opérations de marché.

Comme dans d'autres domaines, « l'interface homme-machine» en tant que tel ajoute une nouvelle classe de risque.

L'absence de sécurité de l'informatique constitue donc manifestement un risque. Aussi les établissements de crédit, qui auront su se préparer à temps pour obtenir un bon niveau de sûreté informatique correctement articulé à un contrôle interne efficient - que la mise en place de l'équivalent formel ou informel d'une notation du niveau de sécurité reconnaîtra - bénéficieront-ils alors d'un avantage concurrentiel incontestable. C'est l'objet de ce livre blanc que de les y aider.

ANNEXE 1 : LETTRE AUX PRÉSIDENTS DES ÉTABLISSEMENTS DE CRÉDIT

Monsieur le président,

Les modalités de fonctionnement des systèmes d'information des établissements de crédit peuvent avoir des conséquences importantes tant pour leur situation propre que pour le système bancaire dans son ensemble. C'est la raison pour laquelle la Commission bancaire est très attachée à ce que le niveau de sécurité des systèmes informatiques soit périodiquement mesuré et que, le cas échéant, les actions nécessaires à son amélioration soient entreprises.

Les règlements du Comité de la réglementation bancaire n° 90-08 et 91-04 relatifs, respectivement, au contrôle interne ainsi qu'à l'organisation du système comptable et au dispositif du traitement de l'information donnent les grands principes qui doivent présider à la bonne organisation et à la sûreté des systèmes d'information.

Dans cet esprit, la Commission bancaire a procédé à une enquête sur la sécurité informatique dont les résultats complets ont été, d'ailleurs, déjà communiqués aux participants et dont la synthèse a été publiée dans plusieurs revues.

À partir des résultats de cette enquête, la réflexion a été poursuivie en liaison avec la profession et a abouti à la publication par la Commission bancaire d'un « Livre blanc » sur la sécurité des systèmes d'information. L'objet de ce document est de présenter l'analyse des principaux risques et les parades possibles ainsi que de formuler des recommandations à destination des établissements de crédit.

L'attention est ainsi appelée sur les principaux problèmes posés par la sécurité des systèmes d'information des établissements de crédit, cette démarche étant d'autant plus utile que la Commission bancaire a parfois l'occasion de constater des insuffisances en ce domaine, préjudiciables au bon fonctionnement des établissements en cause, comme de l'ensemble de la place.

Vous trouverez ci-joint, en annexe, une synthèse du contenu de ce Livre blanc ainsi que son sommaire.

Je vous prie de bien vouloir agréer, Monsieur le président, l'assurance de ma considération distinguée.

Paris, le 7 février 1995 Le secrétaire général de la Commission bancaire

Signé :

J.-L. BUTSCH

ANNEXE 2 : SYNTHÈSE DU CONTENU DU LIVRE BLANC SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les systèmes d'information, et notamment leur support informatique, peuvent constituer une menace financière réelle pour les établissements de crédit.

C'est pourquoi, à la suite d'une enquête menée il y a deux ans auprès d'un échantillon représentatif - et dont les résultats ont été portés à la connaissance de la profession -, la Commission bancaire a souhaité diffuser un « Livre blanc sur la sécurité des systèmes d'information ». Réalisé avec l'aide de la profession, ce document se veut un guide des meilleures pratiques ou selon la terminologie anglo-saxonne « a best practice paper ».

Le Livre blanc est articulé autour de quatre chapitres: les constats, la mesure du risque, les parades et les recommandations possibles. Onze annexes, dont certaines très détaillées comme les trente-six fiches conseils par type de risque, viennent compléter l'ouvrage qui comporte en tout 230 pages.

Les principaux enseignements que l'on peut en tirer sont les suivants.

La Commission bancaire estime que la définition des objectifs généraux de sécurité incombe à la direction générale de chaque établissement de crédit. Pour assumer pleinement sa responsabilité, la direction générale doit connaître avec suffisamment d'exactitude le degré de sûreté de son système d'information, définir le niveau de sécurité qu'elle juge souhaitable par rapport aux exigences des métiers de l'établissement, déterminer les grandes lignes d'une politique de renforcement ou de maintien de la sécurité et se faire rendre compte des résultats des plans d'action qui ont été jugés nécessaires par elle pour les rendre appropriés au degré choisi de sûreté du système d'information de l'établissement. La direction générale doit également s'assurer que le niveau de sécurité qu'elle a ainsi retenu lui permette d'atteindre ses objectifs malgré la survenance de sinistres ou de dysfonctionnements graves et prolongés. Elle doit avoir, enfin, désigné une ou plusieurs personnes pour mettre en oeuvre les modalités pratiques destinées à maintenir ou améliorer la sûreté de son système d'information.

D'une façon plus précise, les questions fondamentales auxquelles il paraîtrait souhaitable d'apporter une réponse sont les suivantes.

- Les objectifs de sécurité informatique de l'établissement sont-ils définis, formalisés et communiqués à tous les collaborateurs concernés ?

- Un collaborateur direct a-t-il été désigné pour assumer la fonction de « responsable de la sécurité du système d'information » (RSSI) de la maison?

- Les points éventuels de vulnérabilité informatique ont-ils été déterminés et les pertes directes ou indirectes qu'ils pourraient occasionner sont-elles mesurées?

- « Le risque maximal tolérable » (RMI) - défini comme la proportion des fonds propres fixée comme limite à ne pas dépasser pour ne pas remettre en cause la pérennité de l'établissement face à un sinistre informatique majeur - est-il connu ?

- Dans quel délai d'autres mécanismes de circulation de l'information vous permettraient-ils de reprendre une activité normale, en cas d'indisponibilité durable du système informatique?

L'objet de ce Livre blanc est de tenter d'aider tous les établissements à apporter des réponses concrètes à ces questions.

ANNEXE 3 : SOMMAIRE DU LIVRE BLANC SUR LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

2. Une menace financière réelle

3. Quelques exemples concrets des menaces dues aux systèmes d'information

II. LA MESURE DU RISQUE

1. Un exemple: l'enquête menée par le secrétariat général de la Commission bancaire en 1992

a. une enquête pour servir de base de référence
b. un impératif : sensibiliser au plus haut niveau
c. un mini-questionnaire: soixante-cinq questions pour cerner la sécurité
d. évaluer les contraintes (budgétaires, d'assurances)
e. apprécier la satisfaction des utilisateurs et le niveau d'efficacité/qualité de l'informatique
f. conclusion: au total, une sécurité informatique globalement satisfaisante, mais perfectible

2. Une méthode formalisée de mesure du risque: quelques conseils

a. connaître ses risques
b. classer ses informations en fonction des quatre facteurs de sécurité DICP
c. évaluer son risque maximal tolérable (RMT)
d. classer ses informations entre stratégiques et non stratégiques (échelle d'évaluation de l'impact des risques)
e. mesurer ses faiblesses (mini-questionnaire Marion)
f. comment arbitrer entre les priorités?

III. LES PARADES POSSIBLES

Les trois niveaux de réponse

1. Niveau 1 : réduire les faiblesses découvertes

2. Niveau 2 : passer d'une réponse au « coup par coup » à une réponse organisée:

a. désigner un responsable de la sécurité du système d'information, faire un schéma directeur
b. les cinq conditions de sa réussite

3. Niveau 3 : agir en prévision des risques nouveaux

IV. RECOMMANDATIONS

1. pour les RSSI (responsable de la sécurité du système d'information)

2. pour les dirigeants responsables

3. Les points de sécurité les plus importants

CONCLUSION

- Le risque informatique est une des composantes du risque global de la banque
- Il doit donc être mesuré, surveillé, géré, réduit au mieux
- La direction générale en est, in fine, responsable
- Ceci est faisable
- Il est fortement suggéré aux établissements de crédit de s'inspirer des recommandations contenues dans ce Livre blanc
- Transformer la diminution du risque en arme commerciale
- Vers un « rating du niveau de sécurité informatique »?
- La « constellation du risque bancaire »

Annexes au livre blanc

Annexe I : Lettre envoyée par le secrétaire général de la Commission bancaire aux présidents des établissements de crédit

Annexe II : Textes réglementaires

Annexe III : Questionnaire simplifié

le mini-Marion utilisé dans l'enquête
Matrice de pondération
Quelques résultats

Annexe IV : 36 fiches conseils (types de risques)

- définition
- risques
- parades
- critères de qualité

Annexe V : Les risques, les facteurs de sécurité et les méthodes d'analyse du risque (un exemple)

Annexe VI : La prise en compte de la sécurité dans les applications un exemple: ISM

Annexe VII : Exemple de charte de la sécurité de l'information

Annexe VIII : Le RSSI: sa fonction

Annexe IX : Méthodes utilisables par le RSSI

Annexe X : Renseignements pratiques

- éléments bibliographiques
- adresses utiles
- glossaire

Annexe XI : Liste des participants