Couvrir les risques informatiques : au-delà des solutions techniques

Si la sécurité du système d'information est aujourd'hui désignée comme une priorité, elle ne peut se gérer au travers des seules solutions techniques, mais doit intégrer d'autres critères comme celui du maintien des savoir-faire. Il en va de même pour la gestion des autres facteurs de risques qui touchent les systèmes d'information, comme la rationalisation des fonctions support, l'automatisation des processus, la gestion des crises ou les migrations technologiques avec l'exemple significatif des legacy applications. La maîtrise du système d'information intègre ainsi une nouvelle fonction : celle de la gestion des risques.

THOMAS DE BELLAIGUE
Président-directeur général
Synagir

HERVÉ RATSIMIHAH`
Directeur de missions
Synagir

Au-delà des solutions techniques de sécurité qui inondent le marché et font l'objet de discussions continuellement et largement portées par les événements et les médias, il nous a paru important de rappeler l'importance de la dimension humaine dans la gestion des risques informatiques.

Parce que le système d'information n'est pas uniquement constitué de composants informatiques mais qu'il a besoin de compétences et de savoir-faire pour fonctionner, nous proposons de présenter les réflexions issues des analyses des risques menées par différents projets touchant à l'organisation. Les rapprochements d'activités, l'externalisation, les projets d'automatisation, le plan de continuité d'activité, la gestion de la crise ou les projets de migration technologique sont autant de sujets sur lesquels l'analyse des risques a montré l'importance de dépasser le cadre purement technique pour s'intéresser à d'autres formes de risques.

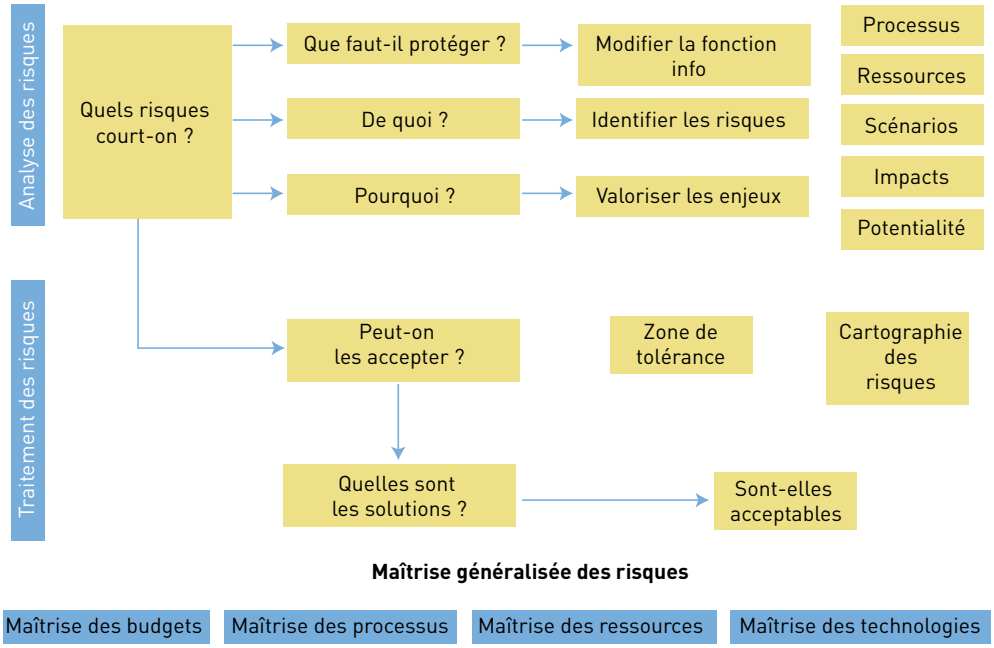
> « L'entreprise prend un risque fort d'arriver à terme, à la mise en place de solutions redondantes, voire incompatibles entre elles. »

La perception du risque informatique

De simple préoccupation, la sécurité ou plutôt le management de la sécurité est entré comme une fonction à part entière au sein des organisations des entreprises et en particulier dans le domaine bancaire où la réglementation impose cette évolution. La fonction de responsable sécurité des systèmes d'informations (RSSI), les schémas directeurs de sécurité informatique, la gestion de budget sécurité dédié, sont les premiers éléments distinctifs de cette prise de conscience.

Les entreprises ont déjà massivement investi dans la protection de leur système d'information : depuis quelques années, les ventes de solutions anti-virales, de Virtual private network (VPN), de Single sign-on solution (SSO), de *firewalls*, de tests d'intrusion et autres solutions de « haute disponibilité » ou de protection de données ont largement contribué à l'explosion du marché de la sécurité. Si le contexte extérieur à l'entreprise contribue à la promotion de ces ventes (les attaques de crackers et les vulnérabilités des systèmes sont largement et fortement mé-

1. Démarche d'analyse et traitement des risques



diatisées), des relais internes à l'entreprise amplifient ce mouvement : les directions informatiques influent plus sur les choix sécuritaires que les directions opérationnelles, en tirant à elles une part importante du budget sécurité – qui s'affiche d'ailleurs en pourcentage du budget informatique –, et en cherchant à copier un « état de l'art technologique ».

Le marché de la technologie contribue lui-même à cette course à l'« armement sécuritaire » en fournissant périodiquement de la puissance pour répondre à des besoins, mais en fournissant aussi les moyens de les contourner : la surenchère des algorithmes de cryptage sophistiqués et le « cassage » des clés en sont l'illustration parfaite.

Le risque de solutions redondantes, voire incompatibles

Si l'impact des risques reste réel et justifiable, la démarche « solution » apporte aussi son lot d'incohérences : si l'entreprise admet volontiers qu'aucune solution n'apporte une protection à 100 % (voire que la solution mise en place est obsolète six mois plus tard), elle perçoit difficilement que sa mise en place peut aussi être la source d'autres failles de sécurité. En forçant le trait sur l'alignement coûte que coûte à l'état de l'art technologique, l'entreprise prend un risque fort d'arriver, à terme, à la mise en place de solutions redondantes, voire incompatibles entre elles, sans prendre le temps d'approfondir les besoins et la valeur du risque, et sans s'intéresser aux autres ressources essentielles à protéger.

« L'automatisation à outrance des traitements s'intéresse aux cas normaux, mais néglige souvent les risques sur le traitement des cas atypiques et leurs impacts sur les charges de travail du personnel. »

« Répondre à un besoin » et « s'assurer de la cohérence des solutions », telle est la logique qui doit présider à la mise en place de toute solution. Si cette logique est bien appliquée aux projets informatiques et aux projets d'organisation, elle s'illustre de plus en plus dans le domaine de la sécurité par l'application d'une méthodologie d'analyse des risques qui s'appuie sur des référentiels, des démarches, des outils et des guides de bonnes pratiques (encadré 1). L'analyse des

risques dépasse le simple cadre d'analyse des ressources techniques en l'agrandissant à d'autres volets (encadré 2) : négliger ces volets, c'est laisser l'entreprise en risque face à la dégradation d'une situation qui, d'une perte financière maîtrisable, pourrait engendrer la perte de clients, voire d'activités beaucoup plus dommageables pour l'établissement.

Les enjeux liés à la maîtrise des savoir-faire

Les récents événements portés par les médias focalisent notre attention sur les attaques virales, les risques d'indisponibilité des systèmes, et abondent dans le sens du marché des solutions de sécurité et leur apport bénéfique. Il est vrai que les enjeux financiers sont importants. Une étude sur ce thème a montré les risques que l'indisponibilité des systèmes pendant une heure pouvait engendrer pour un établissement financier :

« Les projets An 2000 et projets Euro ont déjà alerté les directions générales et informatiques sur les enjeux et risques liés à ces applications anciennes. »

- pour la filière de négociation sur les marchés, une perte de 5 à 7 millions d'euros ;
- pour la filière carte de crédit, une perte de 2 à 3 millions ;
- pour les DAB/GAB, une perte de 20 000 euros liée au non-encaissement des frais inter-banques.

Mais si cette focalisation porte essentiellement sur les composantes techniques du système d'information, elle néglige la plupart du temps la dimension humaine et les risques inhérents aux acteurs.

D'autres facteurs de risque à prendre en compte

D'autres projets ont mis en avant des facteurs de risque aussi importants. Les problématiques de fusion d'activités entraînent souvent la rationalisation des fonctions de support, dont l'informatique, avec la fusion des systèmes informatiques, la définition d'une nouvelle organisation qui nécessitent d'analyser les synergies et risques à la fois techniques et organisationnels.

L'automatisation à outrance des traitements s'intéresse aux cas normaux, mais néglige souvent les risques sur le traitement des atypiques et leurs impacts sur les charges de travail du personnel. L'exemple du *straight through processing* (STP) dans le secteur financier est tout à fait intéressant : le coefficient de STP d'une société de gestion indique son niveau d'automatisation. Un coefficient de 80 % indique, par exemple, qu'un back-office traite en automatique ses ordres à ce niveau, et qu'il est ainsi dimensionné pour traiter manuellement 20 % des flux.

Que se passe-t-il si le coefficient STP passe de 80 à 70 % ? Une chute de ce type amène à traiter manuellement 30 % des flux. Est-ce que le back-office est prêt à traiter dans les temps le surcroît de travail apporté par ces 50 % de flux en plus ? Sinon, quelles sont les conséquences que l'entreprise aura à subir ?

L'indisponibilité ou la perte d'un homme-clé peut mettre en péril la pérennité d'un projet ou d'une application informatique, en induisant un risque à terme sur la disponibilité du service et en faisant subir à l'établissement les conséquences qui en découlent.

L'organisation de la crise, qui si elle est pensée et dépasse le cadre de la solution technique de repli, met cependant l'entreprise en péril si des situations de crise ne sont pas testées avec les acteurs. La mauvaise conception d'un plan de continuité d'activité d'un établissement a ainsi eu pour conséquence l'indisponibilité du système total pendant trois jours suite à un sinistre, entraînant l'arrêt de l'entreprise.

Le cas des legacy applications...

Les choix de migration de technologies posent les problématiques d'acceptation et d'évolution des compétences existantes. Un mauvais accompagnement au changement peut aussi générer des freins auprès du personnel. Un de nos clients indique que sur son projet de migration de langages, « *une évolution de Cobol vers Java requiert l'assimilation de concepts plus complexes liés à une modélisation différente des processus à implémenter. Pour cette raison, il ne suffit pas de familiariser les programmeurs à la syntaxe de ces nouveaux langages. Il faut également veiller à ce que les analystes, chefs de projets et chefs de groupes comprennent en profondeur ce nouveau mode de conceptualisation, de manière à préserver une bonne relation entre les phases d'analyses et les phases de réalisation. Ce challenge constitue la véritable difficulté du passage d'un langage structuré vers un langage objet* ». Ce dernier point trouve son champ d'application sur les projets de trans-

formation des *legacy applications*.

On entend par *legacy applications*, les applications héritées du passé qui ont conservé un poids suffisamment important au sein du système d'information pour que l'entreprise se pose la question sur la stratégie d'évolution à adopter. Vieilles de plus de 20 ans, développées en interne avec des langages dont Cobol reste la figure emblématique, ces applications ont traversé les années pour continuer à offrir aux entreprises un niveau de service et de fonctionnalité acceptable, mais en faisant souvent des concessions sur la cohérence et sur la conservation de la connaissance du système d'information. Les projets An 2000 et projets Euro ont déjà alerté les directions générales et informatiques sur les enjeux et risques liés à ces applications anciennes, notamment sur les besoins de compétences et le niveau de connaissances plus ou moins formalisé.

Le contexte actuel apporte encore plus de pression : les évolutions réglementaires, les exigences des clients, la réactivité des services proposés par les établissements concurrents, les apports des nouvelles technologies amènent les directions informatiques à s'interroger sur la manière d'aligner ces applications aux contraintes de réactivité, de productivité et d'optimisation des coûts.

… et les risques de transfert de technologie

Pour initier la réflexion sur ce sujet, l'étude d'opportunité doit faire le bilan sur la situation actuelle en mettant en avant la valeur du coût porté par la maintenance, en analysant les évolutions et leurs impacts, le niveau de maturité de l'entreprise sur l'application et l'outil actuels, les risques encourus par l'organisation, notamment sur la perte de connaissance. L'étude doit également donner des pistes sur les cibles et solutions possibles en qualifiant les gains en termes de productivité et de coût. Elle doit analyser la capacité de l'organisation à accepter et à s'approprier le changement de technologie. L'étude conclut en final sur la pertinence d'assurer ce transfert : un coût de maintenance supérieur à 30 % au coût de remplacement, une pyramide de compétences limitant à cinq ans l'horizon de stabilité des savoir-faire, un rapport de 1 à 10 sur les charges de développement entre l'outil actuel et l'outil cible sont autant d'éléments qui ont présidé au choix fait par des établissements de lancer au plus tôt leur projet d'évolution.

La solution de l'infogérance

Parmi les solutions retenues par les entreprises, beaucoup ont choisi de regarder si des solutions marché permettaient de couvrir les besoins de leur activité en sacrifiant leur traitement de différenciation. D'autres ont porté leur choix sur le transfert de leur application vers des entités externes : on parle ici d'infogérance et des développements offshores pour la refonte du système. On trouve sur ce type de marché des centres de compétences concentrant des équipes capables de maintenir ou d'assurer le transfert d'applications en Cobol vers les nouveaux standards du marché. À l'origine développé en Inde, ce marché est en train

2. Volets d'analyse des risques sur les ressources informatiques

Composant	Contenu	Critères de risques
Prestations	Services rendus et prestations fournies par la fonction informatique	Qualité, performance, niveau de satisfaction, réactivité, disponibilité
Technologies	Architecture, systèmes, applications, données, réseau	Pérennité, disponibilité, intégrité, confidentialité, traçabilité
Processus	Activités d'étude, de développement, de maintenance, de support, de déploiement, d'exploitation	Qualité des livrables, respect des délais, satisfaction, erreurs/incidents
Savoir-faire	Organisation des connaissances et des compétences sur les technologies et les processus	Maintien et diffusion des compétences, disponibilité des équipes
Budget	Coûts des projets, coûts des infrastructures	Respect des budgets

de se déplacer dans les pays d'Europe de l'Est et d'Afrique du Nord, pour s'ouvrir à la Chine. Les raisons de ce déplacement sont la saturation des ressources et la montée des prix dans les pays à l'origine de ces développements, qui doivent répondre à la fois aux sollicitations « externes » et aux demandes internes en croissance sur leur propre marché.

Une meilleure urbanisation des systèmes

Enfin, d'autres établissements parient sur une meilleure urbanisation de leur système en isolant les composants dans une logique de représentation du système à trois niveaux : deux niveaux correspondent à la collecte et la restitution des informations et sont sujets à des évolutions fortes en termes de services, de fonction, d'ergonomie ; un niveau de traitement entre comme le cœur de l'activité et fige sur un horizon moyen et long terme les règles de gestion et les procédés propres à l'entreprise. La migration d'une *legacy application* s'entend alors comme un découpage de l'application sur ces trois niveaux, et une évolution des niveaux de collecte et de synthèse sur de nouvelles plateformes. Cette solution s'inscrit également dans une logique de mutation en douceur des technologies et des ressources humaines.

« La prise en compte du capital humain constitue un nouvel angle d'analyse qui vient compléter les tableaux de bord existants. »

La mesure des risques sur la maîtrise des savoir-faire

Les directions informatiques sont déjà assez avancées en matière de pilotage : elles sont très fortement équipées de tableaux de bord utilisant des indicateurs de production et de disponibilité des systèmes informatiques. Les évolutions réglementaires liées à Bâle II incitent les établissements financiers à se doter de dispositifs complémentaires, comme les bases incidents, pour suivre, traiter et capitaliser sur les événements porteurs de risques, mais également pour déterminer la valeur des fonds propres. La prise en compte du capital humain constitue un nouvel angle d'analyse qui vient compléter les tableaux de bord existants, et parfaire ainsi la maîtrise globale du système d'information.

La définition des indicateurs de maîtrise des savoir-faire dépend de la perception et de la sensibilité de l'entreprise aux risques sur ses ressources humaines. Face à un risque de perte de compétences, un établissement financier a mis en place des indicateurs sur la pyramide des âges pour ses compétences clés, sur l'ancienneté et le turn-over de ses postes, sur le positionnement des rémunérations de ses salariés par rapport à un benchmark modèle. Pour garantir la disponibilité de ses compétences pour traiter des situations de crise, un établissement a mis l'accent sur la surveillance des taux de charges de ses équipes et la définition d'un niveau de seuil d'alerte. Pour vérifier la diffusion générale des savoir-faire sur des applications, un autre établissement a mis en place la mesure du niveau de polyvalence de ses équipes sur les applications sensibles. Dernier exemple, pour s'assurer de la bonne réalisation d'un changement de plateforme, un établissement a mesuré ponctuellement la capacité de son organisation à assurer cette démarche et a calculé les coûts sous-jacents. Sauf pour le dernier cas cité, les entreprises impliquées ont pu déceler des dérives qui ont été suivies d'actions limitant leurs conséquences. Dans le dernier cas de figure, en revanche, l'établissement a fait un constat qui l'a conduit à transférer à l'extérieur son risque.

La maîtrise de la fonction informatique passe par la gestion globale des risques

La performance du système d'information se mesure au travers de la productivité des outils et des technologies mises en place, mais aussi au travers de la disponibilité et de l'efficacité des équipes en charge des études, des développements et de l'exploitation informatique. Il en va de même pour la sécurité du système d'information, qui ne doit pas limiter son action à la sécurité de ses seuls composants techniques.

Au-delà de l'alignement aux objectifs stratégiques de l'entreprise et du souci permanent d'utiliser au mieux les ressources dont elle dispose, la maîtrise du système d'information intègre ainsi une nouvelle fonction : celle de la gestion des risques. Cette maîtrise induit la contrainte naturelle d'améliorer les systèmes de pilotage existants en mesurant les niveaux de production et les niveaux d'incidents, mais aussi en élargissant la mesure des indicateurs à l'ensemble des composants du système d'information. ¤