Tribune : « Fraude » à la Société Générale, où est l'inadmissible ?

A l'heure actuelle, les tenants et aboutissants ne sont pas clairement connus, cependant il est possible dès maintenant de s'étonner fortement sur certains points relatés publiquement.

Nous ne sommes plus à la fin des années 80, lorsque les contrôles étaient encore artisanaux. Depuis les affaires Enron ou Worldcom, les procédures de contrôles doivent être analysées, améliorées et régulièrement testées. L'informatique sous-jacente est cruciale à contrôler. La célèbre section 404 de Sarbanes-Oxley est passée par là. Normalement on vérifie l'efficacité opérationnelle des contrôles. Voyons cela de plus près.

La banque a une tradition immuable : personne ne peut faire seul quelque chose de risqué. Les banquiers suisses appellent cela le « principe de quatre yeux ». Aller retirer 200 euros à un guichet en Suisse et vous verrez que deux personnes interviennent. Or, on nous dit que le dénommé Kerviel a agi seul. Première grosse surprise ! Personne ne peut agir seul normalement dans une banque ! Sauf peut-être le balayeur (et encore, en Suisse…).

On peut alors penser que ce qu'il faisait n'était pas considéré du tout comme risqué : deuxième grosse surprise ! Comment la Banque a-t-elle fait son analyse de risque ? Les logiciels utilisés permettent peut-être des contrôles dans le cadre d'une délégation de pouvoir ou de droits. Ces contrôles limitent le risque, dans le cas présent ils sont soit absents, soit inefficaces !

On se dit alors que, puisque c'est ainsi, le trader indélicat a dû cacher le risque : troisième surprise ! On peut donc cacher un risque en le déguisant. Kerviel a, paraît-il, créé des sociétés fictives pour répartir les montants en jeu. Là aussi surprise ! Le logiciel ne contrôle pas l'existence des sociétés créées? Une rapide interrogation dans un fichier Insee ou équivalent aurait pu faire l'affaire, ou encore une demande de validation par un collègue. Il y a là une faiblesse dans l'informatique si cela est vrai !

On se demande alors si le logiciel en question n'aurait pas été reparamétré pour désactiver les contrôles gênants. La question se pose alors : par qui ? Un informaticien ? Ils seraient alors deux dans la fraude. Si l'on nous dit que Kerviel a fait tout cela seul, il faut se rendre à l'évidence : l'utilisateur Kerviel a pu modifier des paramètres importants en production bancaire. Carton rouge ! C'est une règle de base en informatique (et pas que dans la Banque cette fois-ci) aucun utilisateur ne peut modifier des paramètres en production. Tout logiciel sérieux l'interdit d'ailleurs. Les logiciels employés dans cette affaire seraient-ils des produits non sérieux ? Là encore une approche de type SOX404 ou encore Cobit doit vérifier cela !

Reste alors le meilleur, gardé pour la fin : c'est parce qu'il connaissait les contrôles, qu'il a pu les contourner ! Autrement dit, la force du contrôle est d'être secret ! La sécurité repose donc sur un système instable car rien ne peut rester secret, surtout pas des procédures de contrôle, qui doivent être l'objet de tests et d'audit régulier. Par ailleurs, ces procédures ont des failles : comment se fait-il qu'elles n'aient pas été identifiées ?

De quelque bout que l’on prenne cette affaire, on aboutit fatalement à des manquements graves. L’étude des risques et contrôles informatiques semble absente !

___

(*) Consultant, Duquesne Research