RAPHAËL MARICHEZ (2002) *fonctionnaire de la sécurité des systèmes d'information (FSSI), ministère de l'Intérieur*

SÉCURITÉ DES SYSTÈMES D'INFORMATION : LA NÉCESSAIRE CLARIFICATION DES RÔLES

Le rôle du « responsable de la sécurité des systèmes d'information » (RSSI) est très mal défini. Parfois craint, parfois rejeté, il suscite l'intérêt lorsque surviennent des cyberattaques. Une clarification de son rôle et la mise en place d'une gouvernance collégiale de la sécurité sont indispensables pour assurer une vraie gestion des risques liés aux systèmes d'information.

Le RSSI n'est certainement pas « responsable » du niveau de sécurité informatique atteint par la structure qu'il représente. Le vocable même de RSSI trompe le dirigeant, qui, victime de l'illusion de pouvoir se reposer sur une seule personne ou équipe, se désintéresse du sujet.

L'ILLUSION DU TRANSFERT DE RESPONSABILITÉ

Lorsque les choses vont mal en matière de systèmes d'information, c'est bien auprès du DSI que les autorités cherchent des explications et des solutions. Après tout, l'essentiel des dispositifs de traitement, de diffusion ou de protection de l'information relèvent du système d'information proprement dit : les réseaux informatiques, les ordinateurs, les logiciels. Si les secrets commerciaux sont captés par la concurrence lors d'un piratage informatique, il serait difficile d'en attribuer la responsabilité au seul directeur commercial.

« La fonction SSI relève davantage d'un processus que de l'incarnation d'un pouvoir »

DES RESPONSABILITÉS IMBRIQUÉES

En pratique, le RSSI est un rouage d'une plus vaste structure transversale au sein de laquelle les responsabilités sont fortement imbriquées. Penser que le RSSI pourrait être comptable du niveau de sécurité, et donc des incidents et des préjudices subis, crée une distorsion néfaste au fonctionnement efficace de l'organisation : soit en concentrant exagérément les moyens et le pouvoir auprès d'une personne ou d'une équipe, soit, beaucoup plus souvent, en déresponsabilisant les autres parties prenantes de l'entreprise à l'égard du risque SSI. La fonction SSI relève davantage d'un processus que de l'incarnation d'un pouvoir quelconque : un processus de gestion des moyens (financiers, techniques, humains), des risques, des coûts de la sécurité et de ceux de l'absence de sécurité. Ce processus doit idéalement irriguer de manière continue et homogène toute la structure jusqu'à ses interfaces, des actionnaires aux utilisateurs finaux. C'est pourquoi la protection et la défense des SI doivent être pensées dans leur ensemble et en lien avec les métiers, au risque, sinon, de menacer la structure entière à cause d'une seule défaillance localisée.

DES MOYENS GÉRÉS PAR LA DIRECTION DES SYSTÈMES D'INFORMATION

Puisque le DSI est sans nul doute le principal responsable du bon fonctionnement des systèmes d'information, il semble naturel, en première approche, que la fonction de pilotage de la SSI et des risques associés s'incarne en son sein. Le RSSI a donc longtemps été en charge de la mise en œuvre de briques de sécurité technologique nécessaires au bon fonctionnement des systèmes. Mais, aujourd'hui, il doit agir en liaison avec la gestion des risques métier réels.
La sécurité des SI ne se limite plus, en effet, au seul bon fonctionnement du système :

REPÈRES

RSSI pour responsable sécurité des SI, DSSI (directeur) ou FSSI (fonctionnaire), ou RSSI-groupe, RSSI opérationnel, OSSI (officier SSI)... Malgré les efforts des réglementations administratives ou internes aux compagnies privées, le rôle et les missions de ces acteurs en charge de la sécurité des systèmes d'information ne peuvent cependant pas être référencés sous un vocabulaire interchangeable. Leur activité au quotidien dépend étroitement de leur environnement professionnel immédiat, de la culture et des priorités de l'entreprise.

© LEKKYJUSTDOIT / FOTOLIA

La tendance est à la recherche de sécurité *by design*.

il faut compter avec l'espionnage économique, l'altération invisible des paramètres du système, le chantage au sabotage ou à la divulgation massive de données.

LES LIMITES D'UNE APPROCHE BUDGÉTAIRE

Les métriques les plus faciles à utiliser pour jauger du degré de prise en compte de la sécurité dans les SI reposent évidemment sur le budget. Les études publiées exposent une part de dépenses consacrées à la sécurité de l'ordre de 6 % à 12 % du budget des systèmes d'information. Ces chiffres masquent des réalités fort variables selon la façon de prendre en compte les dépenses. Aujourd'hui, la tendance est à la recherche de la sécurité *by design*, fondue au sein du produit, comme lorsqu'on achète une voiture sans se poser la question de la part du prix liée à l'airbag ou à l'ABS. La généralisation, notamment dans le monde anglo-saxon, des mécanismes de couverture du risque par des mécanismes de mutualisation (assurances) favorise cette tendance à la contractualisation d'une garantie de sécurité, notamment par le truchement de la certification de produits (critères communs), ou de processus (ISO 27001).

« Le RSSI devient à la fois un stratège et un lobbyiste »

PILOTER LA SÉCURITÉ PAR LES RISQUES MÉTIER

Le pilotage moderne de la sécurité des systèmes d'information, ou plus exactement du risque lié à la (non-)sécurité, s'inscrit plus aisément dans la logique verticale de l'appareil productif de l'entreprise : le responsable de la *business unit* doit être amené à arbitrer le bon niveau de sécurité, au regard de ses enjeux métier propres, à la lumière d'une expertise avisée en matière d'évaluation des risques circonstanciés au métier. Le RSSI moderne est donc un expert et conseiller, apte à vulgariser le risque d'origine informatique qui pèse sur l'activité métier, force de propositions pour réduire ce risque, pilote des actions associées.

Cette démarche vise finalement à trouver un juste compromis entre risques, moyens de sécurité et priorités opérationnelles.

Les qualités d'expertise, de pédagogie, d'ouverture d'esprit, et la force de conviction du RSSI sont fondamentales. Le responsable métier (maître d'ouvrage) doit pouvoir s'appuyer avec une confiance quasi totale sur son RSSI, dans un monde technique au vocabulaire incompréhensible, face à une ou plusieurs DSI confrontées à leurs propres enjeux, face aux prestataires et fournisseurs, face aux clients indécis, face aux autorités réglementaires exigeantes, le tout sous contraintes de moyens et de calendrier. Cette confiance ne se décrète pas par un titre, mais se gagne au mérite.

ARBITRER LA SÉCURITÉ DANS LES APPLICATIONS TRANSVERSES

Dès lors qu'un système d'information, généralement de soutien (messagerie, réseau, hébergement, bureautique, téléphonie, etc.) est transversal aux différents métiers, le juste équilibre entre investissement et bénéfice est beaucoup plus difficile

à déterminer. Les différentes populations bénéficiaires n'ont en effet pas la même appétence au risque : chacune n'est pas prête à contribuer au même niveau à l'effort collectif. L'arbitrage devient délicat.
Dans le domaine des systèmes d'information transverses, les méthodes de gestion des coûts de soutien mutualisés, et, à travers elles, les méthodes d'arbitrages des projets de sécurisation des SI, constituent aujourd'hui un domaine d'exploration et de recherche passionnant. Le RSSI appréhendera les mécanismes budgétaires et décisionnels de sa structure afin d'orienter les efforts de sécurité dans la direction qu'il pense être la plus adaptée : il devient à la fois un stratège et un lobbyiste.

DIFFUSER UNE CULTURE DE CYBERSÉCURITÉ

La fonction SSI moderne s'oriente vers des actions de long terme, influençant lentement les habitudes de travail et les structures décisionnelles au sein de l'entreprise. C'est ainsi tout naturellement que cette fonction SSI se rapproche étroitement de celle d'un communicant, voire d'un « évangéliste » : sensibiliser, former, promouvoir, diffuser et infuser, vendre la sécurité en interne, ainsi qu'auprès des clients, fournisseurs et partenaires, jusque dans les comportements de la vie privée, afin d'impulser le changement.
Cette activité est en concurrence avec d'autres activités transversales non moins légitimes : politique sur le handicap, sécurité incendie, développement durable, etc. En outre, son efficacité est extrêmement difficile à mesurer. C'est pourquoi il s'agit très certainement de la tâche la plus difficile du RSSI, du reste rarement formé aux techniques de la communication et du marketing.

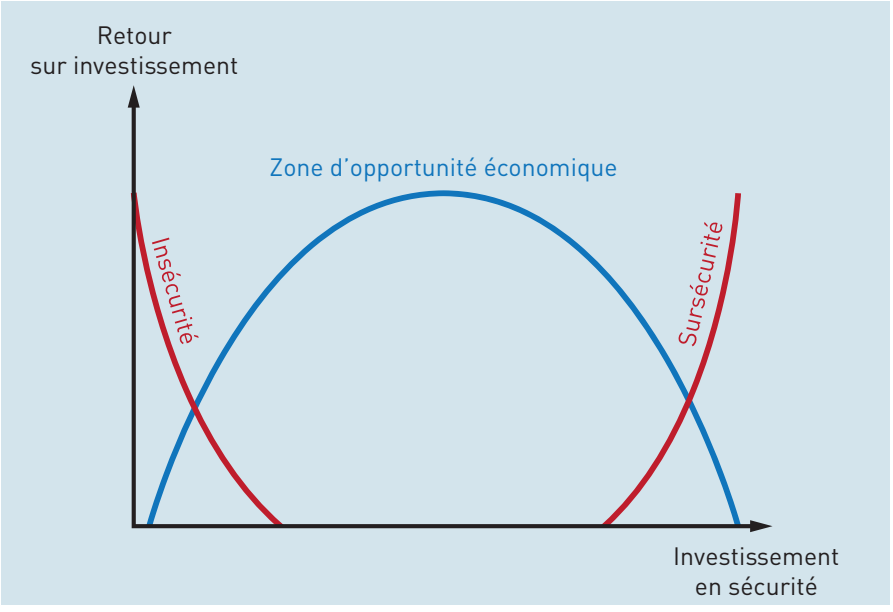
GÉRER LES CRISES

Parmi les leviers de la communication, la capitalisation sur les incidents de sécurité, voire les crises, est un atout évidemment essentiel à exploiter. Cette capitalisation ne peut compenser à elle seule les coûts et préjudices liés à l'incident, mais exige néanmoins une préparation en amont trop souvent oubliée, notamment en matière d'indicateurs sur les impacts des incidents (RH consommée, perte d'exploitation, coût des investigations et de la reconstruction).
L'acteur de la SSI doit être au cœur de la gestion de la crise cyber, sauf à s'interdire d'exploiter une formidable caisse de résonance : la proximité avec les responsables métier, l'indépendance complète à l'égard de la DSI, l'attention de la part de la haute hiérarchie sont autant de facteurs, qui, bien qu'éphémères et simultanés, favorisent la capacité du RSSI à convaincre pour impulser des changements significatifs dans les habitudes, les procédures ou les architectures.
Le volet communication ne doit pas rimer pour autant avec gesticulation. Un grand doigté est requis pour gérer les attentes, souvent irrationnelles et éphémères de l'échelon supérieur (quel pays nous attaque ? pour quel motif ? quand pourra-t-on reprendre une vie normale ?) et en tout cas sans lien avec les actions à mener en résolution de crise (exploiter les traces, reproduire le chemin d'attaque voire l'anticiper, prioriser les RH disponibles, sacrifier des systèmes, tenir une main courante et faire circuler l'information).
Bien qu'évidemment non souhaitable, une crise bien préparée et bien gérée est un formidable outil de sensibilisation et de collecte de métriques au profit du pilotage de la SSI dans sa globalité.

« Communication ne doit pas rimer avec gesticulation »

CHERCHER LE BON COMPROMIS ENTRE COÛTS ET EFFICACITÉ

En aval du marketing interne de la SSI, les actions variées d'un acteur de la SSI, qui serait économiquement rationnel, concourent finalement toutes à un objectif de maximisation des effets positifs de la SSI sur le *business*, évidemment, sous contrainte des moyens alloués.
Faut-il en effet s'efforcer de trouver (et de prouver) le graal du RSSI, le « retour sur investissement (ROI) de la sécurité » ? J'ai expliqué la grande difficulté à calculer le coût de la sécurité. Évaluer objectivement le coût de la non-sécurité (perte d'exploitation, gestion de l'incident, reconstruction, sans compter



DR

Il est difficile de définir le niveau de sécurité économiquement optimal, mais le RSSI doit s'efforcer de s'en rapprocher en moyenne.

© MIMADEO / FOTOLIA

Diriger les moyens disponibles de la meilleure façon qui soit.

le préjudice invisible comme l'espionnage économique) est certainement encore plus utopique, surtout au milieu d'une gestion de crise. L'extrême volatilité de la probabilité d'occurrence du sinistre ne milite pas non plus en faveur d'une approche de type assurance du risque cyber : la fréquence des cyberattaques sur des sites Internet français a par exemple connu une explosion sans précédent la semaine ayant suivi les attentats de *Charlie Hebdo*. Pour ne rien arranger, les statistiques de sinistralité dans ce domaine ne dépassent évidemment pas quelques années d'historique.

Au lieu de tenter de calculer en vain un ROI crédible, une autre approche est possible : simplement diriger les moyens disponibles de la meilleure façon qui soit, en proscrivant les extrêmes, et en recherchant une certaine homogénéité du niveau de sécurité au sein d'un périmètre de sensibilité homogène. Il vaut généralement mieux s'attacher à fiabiliser un système de chiffrement de données partagé (par exemple : HTTPS) plutôt que d'ajouter une surcouche de chiffrement applicatif spécifique au projet.

Ce pilotage optimal des moyens alloués (ou allouables) à la sécurisation des SI, au sens large, doit être la ligne de conduite permanente du RSSI. Celui-ci doit ainsi rechercher les leviers d'action, la plupart du temps évidemment sans autorité hiérarchique directe, sur les grandes masses de moyens. Il s'agit tout autant des moyens financiers, humains, que matériels, et tout autant des moyens de pure sécurité (pare-feux, antivirus, sondes, etc.) que des moyens annexes utilisables au profit de la sécurité (systèmes bureautiques, annuaires, cœurs de réseaux, badges avec puce électronique, etc.).

« Le risque cyber est sous-jacent à la gestion du risque lié à l'activité »

INSTAURER UNE GOUVERNANCE DE LA SÉCURITÉ

Le rôle moderne du RSSI, quelle que soit sa dénomination exacte, ne peut donc faire l'économie d'un pilotage transverse de moyens qu'il ne possède pas, au travers de leviers tactiques sur lesquels il n'a aucune prise directe. Comment faire ?

D'une part, la méthode la plus complète repose sur une bonne connaissance de l'existant par les audits et les tests d'intrusion (patrimoine informatique, ou numérique pour les plus avancés, ses vulnérabilités, ses atouts), une gestion-capitalisation des incidents de sécurité, et une gestion des risques à plusieurs niveaux (entreprise, *business unit*, projet) liant le risque porté par le système d'information aux intérêts du projet, du *business*, de l'entreprise.

D'autre part, le « savoir-être » des acteurs mettant en œuvre ces trois processus est indispensable : les qualités de relations humaines, de communicant et de conviction permettent le « management transverse », une espèce de *soft power* influençant les structures de l'entreprise échappant à son autorité hiérarchique. Ces qualités favorisent également la création d'un quasi-service de renseignement interne, absolument nécessaire au travail du RSSI.

VALORISER LA SÉCURITÉ PAR UN VRAI MARKETING INTERNE

Ce portrait d'un RSSI modèle et moderne n'est certainement pas parfait, immuable ni absolu. Il traduit une vision répondant aux besoins actuels des grandes organisations de culture francophone, et au constat malheureux d'un véritable divorce entre le RSSI et les bénéficiaires de son action en entreprise ou en administration. La faute est largement partagée : trop rares sont les RSSI qui prennent le temps d'aller rencontrer les « métiers » pour « vendre » de la sécurité qui corresponde à leurs besoins, trop rares sont les dirigeants qui acceptent de perdre en confort pour protéger le patrimoine de la société.

La cybersécurité en entreprise ou en administration est résolument à la confluence de la gestion du risque opérationnel et du numérique, dont le système d'information est le socle. De même que les géants du Web tirent leur prodigieuse efficacité de l'intégration verticale des composantes du numérique (du dimensionnement de la fibre optique transatlantique au modèle économique de diffusion du contenu en Europe), les dirigeants publics et privés doivent intégrer le risque cyber comme un sous-jacent de la gestion du risque lié à l'activité qu'ils dirigent, risque dont la responsabilité leur incombe *in fine*. ■