Auteur : Kamal HAJJOU
Consultant Manager sécurité systèmes d'information

Gouvernance et sécurité des systèmes d'information

Stratégie, règles et enjeux

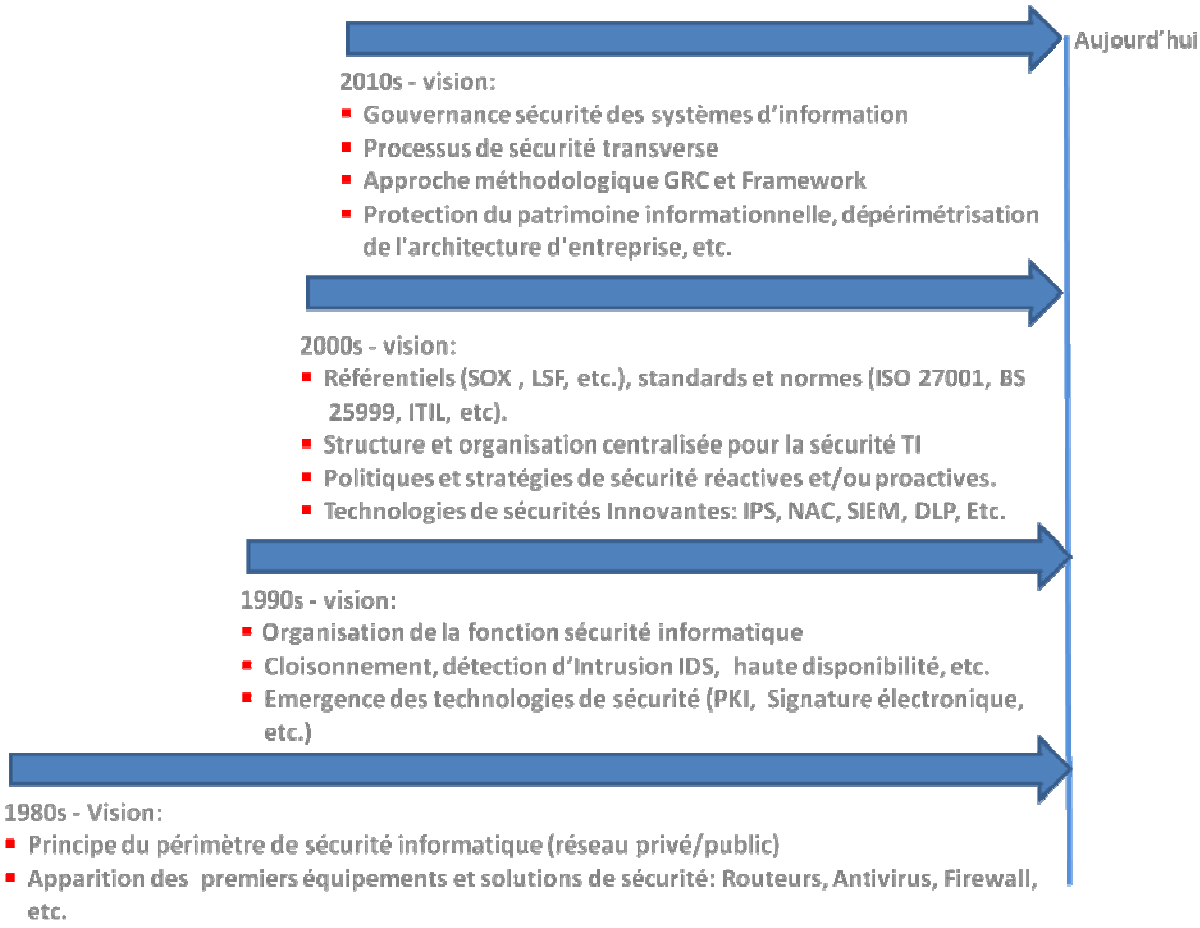
Avant- propos:

Cet article tente de dresser un état des lieux sur les approches préconisées pour sécuriser les systèmes informatiques, initier une réflexion sur les limites des visions traditionnelles adoptées, louer l'importance de la gouvernance de la sécurité des systèmes d'information comme approche globale et proposer quelques pistes pour réussir le programme de sécurité SI de votre organisation. Si le sujet vous interpelle, n'hésiter pas de me faire part de vos questions et réactions.

Vision et stratégies:

L'économie numérique est devenu le principal levier de l'économie mondiale, face à ce constat le rôle des centres de données est primordial, ces usines des temps modernes centralisent l'informatique de toutes organisations, entreprises, etc. Ils sont la clé de voûte pour la création de la valeur, et leurs indisponibilités à un impact humain et financier indéniable.

Les enjeux de la sécurité des systèmes informatiques représentent un défi majeur qui se résume à l'impossibilité de donner des détails, car l'environnement et la technologie changent constamment, ce qui nécessite un changement de vision.



Pour faire face aux risques informatiques, les organisations multiplient les couches de sécurité : double pare-feu périmétrique, IPS, PKI, NAC, anti-virus de postes/serveurs...., une approche réactive nécessaire mais insuffisante pour contrer par exemple un contournement passif initié par l'utilisateur sans vouloir nuire intentionnellement à son entreprise.

Des stratégies proactives sont souvent adoptées par l'organisation pour assurer la résilience de son système informatique, par la mise en place d'un PCA (Plan de Continuité d'Activité) orienté activités métiers et/ou des PRA (Plan de Reprise d'Activité) orienté infrastructures technologiques, ou par l'utilisation d'un Cloud privé ou public qui permet d'externaliser des applications/métiers vers un opérateur pour résoudre les problèmes de la sécurité (attaque virale, intrusion...). La pertinence et l'efficacité de ces approches sont étroitement liées aux respects des niveaux de services et au maintien opérationnel des exigences de sécurité, d'où l'importance d'un contrôle permanent de la sécurité SI.

Néanmoins, il est nécessaire de rappeler que le risque informatique est un risque global, en raison de l'interconnexion des économies et des réseaux TI, les organisations doivent faire face à la **guerre de l'information** ou cyberguerre**,** cette réalité est décrite par le Pentagone comme le cinquième domaine de guerre, puisqu'il reconnait l'importance égale du cyberespace par rapport à l'espace territorial, maritime, aérien et spatial pour les opérations militaires. Les cyber-terrorismes sont devenus une menace persistante (Advanced persistent threat), les vers flame ou stuxnet constituent un parfait exemple de cette méthode d'attaque, un cas d'école de menace avancée persistante.

Dans ce sens, une enquête sur la Gouvernance de la Sécurité Informatique réalisée par L'AFAI, qui date de 2002 mais qui reste d'actualité en raison des problématiques abordées:

- L'évaluation et la perception des risques,
- Les types d'actions de sécurité,
- L'organisation de la fonction SSI,
- Les budgets et les dépenses,
- Le pilotage et le contrôle.

Le résultat de cette enquête, met en évidence une perception de la sécurité souvent réduite au seul domaine informatique, et relève un manque d'une stratégie globale au niveau des entreprises sondées. Certes la sécurité informatique est nécessaire, mais reste insuffisante pour faire face à des risques tels que la cybercriminalité.

Approche méthodologique:

Dans le cadre La gouvernance des systèmes d'information, il est nécessaire d'intégrer une approche globale de la sécurité, qui propose de:

- Donner une vision complète du niveau de sécurité de l'organisation
- Mettre en évidence les écarts par rapport aux objectifs
- Identifier les risques SI
- Identifier les actions correctrices à mener
- Aider à affecter les bonnes priorités aux différents projets

Cette approche globale doit également assurer des prérogatives, à savoir :

- Transparence de l'information

- Accessibilité de l'information
- Fiabilité de l'information et des données
- Sécurité de l'information et des données
- Traçabilité de l'information

La gouvernance de la sécurité des systèmes d'information est une démarche globale, qui adopte une approche GRC (**Gouvernance, risques, Conformité**)**,** soit une vision holistique de l'organisation qui désigne l'ensemble des moyens techniques, opérationnels et organisationnels déployés pour optimiser la gouvernance des systèmes d'information, le management des risques et l'audit des systèmes d'information.

La gouvernance de la sécurité de l'information est clairement **proactive** dans le sens où elle tient d'une volonté de protection du patrimoine de tous les actifs informationnels de l'organisation, c'est une approche «Top Down» notamment par la mise en œuvre de référentiels de sécurité (SOX, normes Bâle II, normes Solvabilité II, ISO 27001, ISO 22301, COBIT, ITIL, etc.). Elle est aussi **réactive**, puisqu'elle assure la mise en œuvre des innovations techniques de sécurité pour contrer les risques informatiques, elle assure également l'évolution de l'architecture d'entreprise pour accompagner les évolutions organisationnelles, managériales et sociologiques de votre organisation, d'où l'importance d'un traitement de l'information en «Bottom-up» guidé par les données, pour effectuer une synthèse des processus informatiques au fur et à mesure qu'il remonte dans les couches fonctionnelles du plus fin (événement « brut ») au plus complexe (information agrégée ou consolidée), dans une optique de protection des systèmes informatiques.

La gouvernance de la sécurité de l'information est un processus transverse qui assure la sécurité des systèmes d'information de votre organisation, qui définit un programme, des activités, et les objectifs de sécurité de l'organisation:

- Définir un cadre de gouvernance de la sécurité SI : stratégies, procédures, outils, documents, etc.
- Définir une politique de sécurité **globale,** qui s'inscrit dans le cadre d'un programme de sécurité SI
- Etablir des objectifs (indicateurs)
- Concevoir un système de management de la sécurité SI (SMSI), pour atteindre les objectifs de sécurité informatiques qui répondent aux besoins de votre organisation
- S'assurer du traitement et du contrôle des exigences de sécurité au niveau organisationnel, fonctionnel, et opérationnel
- Superviser les objectifs de sécurité SI (contrôle et audit)
- Adopter un management du changement et du reporting tout au long du cycle de vie du programme(s) sécurité SI
- Sensibiliser, communiquer, capitaliser.

Ce processus de gouvernance implique la mise en œuvre d'un programme de sécurité SI et d'un management par portefeuille projet, qui garantie une bonne gestion des finances (gestion des coûts des projets), une qualité de la prestation de services (assurant les livrables), et qui contribue à assurer la création de valeur. Cette approche systématique et globale de la sécurité de l'information permet de:

- Conseiller la direction générale sur la meilleure façon de gouverner la sécurité SI
- Identifier les exigences de sécurité SI et les processus concernés
- Réaliser une analyse d'impact métiers efficace est essentielle pour protéger ces actifs informationnels.

- Quantifier la totalité des risques inhérents à l'activité de l'organisation.
- Classifier et hiérarchiser les risques
- Mettre en œuvre un programme(s) d'actions
- Superviser le système de management de la sécurité SI de votre organisation.
- Prévoir une gouvernance spécifique pour faire face aux crises (gestion de crise et communication de crise pour réduire l'impact médiatique des aspects économiques, financiers et sociaux de tous les événements aléatoires qui pourraient survenir).
- Capitaliser, améliorer et valoriser.

La gouvernance de la sécurité de l'information s'articule avec les programmes renforçant la culture de bonne gouvernance SI et s'assure que la politique de sécurité SI de votre organisation a été précédée par et s'articule avec des politiques spécifiques: sécurité de l'information, archivage, gestion des crises, santé et sécurité au travail, tableau de bord juridique, charte de déontologie…, soit une démarche de cohérence et de complémentarité.

Cette approche par programme pour la gouvernance de la sécurité SI implique des décisions stratégiques, qui sont de l'autorité de la direction de votre organisation et du staff management. Une structure de type comité de pilotage de programme(s) ou d'arbitrage est à prévoir pour la prise de décision et le pilotage de la sécurité du système d'information au sein de votre organisation, ce comité est le commanditaire du programme(s) de sécurité SI, dans lesquels les responsables des directions fonctionnelles, techniques, et les parties prenantes de l'organisation sont représentées (Utilisateurs clés, décideurs, DSI, MOA, MOE, etc.). Et on n'oublie pas le RSSI et le CIL.

Le comité de pilotage programme est responsable des prises de décisions stratégiques, il définit la vision de la sécurité à adoptée, l'organisation de sécurité à mettre en place, les critères de gestion du portefeuille de projets sécurité SI, les critères de priorisation, le processus d'amélioration continue de la gouvernance de sécurité SI, etc. C'est aussi une instance de décision, qui aura plus d'influence sur le sponsor de votre projet, rappelons que le sponsoring de projet à d'autant plus d'impact qu'il vient d'une personne haut placée.

La planification du programme(s) de sécurité doit être évaluée de façon structurée sur la base d'une série de critères en vue de son approbation, le management des projets de sécurité doit être transverse, la gestion des projets de sécurité SI doit être intrinsèquement imbriquée dans une logique métier qui se doit d'être mise en cohérence de façon continue avec les exigences de sécurité TI. L'allocation des ressources entre les différentes catégories de projets est par conséquent du ressort de la gouvernance d'entreprise et ne relève ni de la seule compétence de la DSI et/ou RSSI, ni de sa seule responsabilité.

Le pilotage des projets de sécurité SI au niveau de ce comité, permet une gouvernance d'un point de vue global (domaine du décisionnel):

- Définir la vision et le périmètre
- Définir les exigences de sécurité SI et les critères de contrôles
- Inscrire les bons projets dans le programme sécurité SI
- Prioriser son portefeuille de projets de sécurité SI
- Faire la distinction entre la politique globale et spécifique pour chaque système d'information de l'organisation
- Identifier les cycles d'examen et de révision
- Faire le suivi de la planification du programme de sécurité, et s'assurer du respect des calendriers pour chaque projet de sécurité.

Importance du Framework:

Pour que les entreprises soient plus agiles, les technologies doivent être intégrées aux objectifs stratégiques de l'organisation, l'infrastructure technologique doit fournir un véritable levier pour une plus grande performance organisationnelle et devenir une source importante d'avantages compétitifs. Pour faire face à l'hétérogénéité des systèmes informatiques, la conception pour chaque organisation d'un « Framework » ou selon l'office québécois de la langue « cadriciel », permet d'adopter une approche structurée des préoccupations liées à la gouvernance des systèmes d'information et à leurs sécurités, organisée en fonction des points de vue des acteurs impliqués (métiers, DSI, RSSI, partenaires..), elle permet également:

- Focus sur le métier et intégration des technologies informatiques
- Définit un référentiel de sécurité basé sur les normes, standards et bonne pratiques
- Garantie une confiance des cadres dirigeants
- Fournit un langage commun
- Assure une acceptabilité générale
- Structure et organise avec des responsabilités claires (Matrice RACI)
- Assure une utilisation efficiente des ressources
- Evolution des bonnes pratiques utilisées
- Permet une veille technologique pour l'entreprise
- Respect de la réglementation
- Atteindre les objectifs de surveillance et de contrôle
- Un meilleur retour sur investissement
- Améliore en continue

Un Framework devrait encourager l'esprit d'équipe et la pensée créative au sein de votre organisation, d'accroître l'efficacité du processus de gouvernance de la sécurité SI, de rationaliser la sécurité informatique et de l'aligner sur les objectifs globaux de l'organisation, et non d'être un cadriciel bureaucratique. Pour ce faire, il est nécessaire que votre Framework soit développé d'une manière qui prend en compte non seulement l'organisation mais les besoins et les opinions de l'ensemble des acteurs, en cultivant un sentiment d'appartenance.

L'implémentation de votre Framework doit permettre d'identifier les processus et les solutions techniques à mettre en œuvre, la structure organisationnelle qui sera adoptée, et les mesures procédurales qui doivent être incorporées.

L'adoption d'un Framework pour votre organisation, est aussi un moyen d'établir une distinction claire entre la gouvernance de la sécurité SI et le management de la sécurité SI. Les deux disciplines comprennent différents types d'activités, nécessitent des structures organisationnelles différentes et servent à des objectives différents. En occurrence, il s'agit de deux comités de pilotage distincts un de pilotage programme et l'autre de pilotage projet.

Cette interaction entre les deux structures organisationnelles, peut être visible dans le cadre de projets de conformité SI majeurs engageant votre organisation (SOX, PCI DSS, ISO 27001, respect des exigences de continuité d'activité de Bâle II, etc.), avec un comité de pilotage du programme pour l'ensemble des projets de conformité SI, et un comité de pilotage pour chaque projet de conformité SI, redevable des prises de décisions opérationnelles. La démarche suivante est donnée à titre d'exemple, elle permet de renforcer le propos:

- Réunion du comité de pilotage du programme conformité SI
- Donner une vision et un leadership
- Approuver le Framework de sécurité SI de l'organisation
- Inscrire les projets de conformité dans le programme conformité SI
- Identifier les exigences de sécurité, les risques et les enjeux.
- Valider le modèle organisationnel de ressources pour le programme conformité SI
- Développer des matrices RACI pour la responsabilité, élaborer des scénarios, avec avantages et inconvénients du modèle de ressources spécifiques à chaque scénario.
- Obtenir l'approbation pour l'affectation des ressources transverses
- Obtenir l'approbation du comité de pilotage projet de chaque projet de conformité SI (stratégies, planning, affectation des ressources, etc.)
- Faire du reporting, et vérifier les résultats
- Effectuer une évaluation rigoureuse: réévaluation des plannings, des compétences, des processus, de la formation, de la communication, de la technologie, etc.
- Réviser le plan du programme initial et prendre les mesures adéquates
- Assurer la rentabilité du programme ((ROI), respect des délais, management des risques, etc.).
- Vérifier si les initiatives actuelles de gouvernance de la sécurité SI génèrent les résultats escomptés
- Démontrer la valeur à travers les résultats obtenus

Le comité de pilotage programme(s) sécurité SI est responsable de vérifier périodiquement, par des missions de contrôle interne ou d'audit, si les objectifs (indicateurs), les processus et les procédures sont:

- Conformes aux exigences de sécurité légales et normes,
- Conformes aux exigences de sécurité métiers,
- Conformes aux exigences de sécurité technologiques et de contraintes

Le rapport d'audit permet de vérifier l'alignement des stratégiques de sécurité adoptées par le comité de pilotage programme(s) sécurité SI aux exigences de sécurité SI de votre organisation, il permet également de vérifier l'efficacité du processus de gouvernance de la sécurité SI et non niveau de maturité, enfin de proposer des recommandations et des actions.

Synthèse :

La gouvernance de la sécurité des systèmes d'information se doit être un enjeu collectif et partagé, qui assure:

- La gestion stratégique de la sécurité SI: structure organisationnelle, planification et alignement/intégration stratégique des technologies de sécurité TI aux exigences métiers et non à la technologie, développement et acquisition d'un système d'information sécurisé, amélioration continue de la qualité et optimisation des coûts des livrables.
- La protection des actifs informationnels: une vision sur les métiers ayant le plus d'impact sur le business de l'entreprise, bonnes pratiques associées à une répartition des efforts, méthodes et référentiels appliqués, protection des ressources informationnelles, problématique de continuité d'activités, etc.
- La gouvernance des risques: identification des risques, classification des risques, avec une bonne compréhension du risque d'exposition et d'une prise de conscience suffisante de la gestion des priorités.
- La conformité répond aussi aux obligations légales et réglementaires : La gestion de la conformité implique l'élaboration de référentiels internes de sécurité qui reposent sur des standards reconnus, les audits de sécurité sous-tendent la politique de sécurité au niveau stratégique comme dans ses déclinaisons au niveau fonctionnel et opérationnel.

La gouvernance et la sécurité des systèmes d'information**,** considère la sécurité des systèmes d'information comme un support de création de la valeur et non plus uniquement comme une contrainte légitime mais pesante, elle à pour objectif de satisfaire les exigences de la haute direction, de s'inspirer des normes, standards et meilleures pratiques pour élaborer un programme de sécurité SI, de mettre en place des structures de négociation et de décisions fondées sur les principes de communication, elle permet d'expliquer aux acteurs les enjeux de la sécurité pour votre organisation, de concilier les visions, de réunir les acteurs autour d'un minimum d'échanges sur les risques SI, d'harmoniser les actions, d'évaluer et contrôler les actions réalisées, enfin elle permet un compromis indispensable pour assurer une sécurité efficiente de votre système d'information.

Pour tous ceux qui souhaitent me contacter, kamalhajjou@gmail.com

Vos suggestions, questions, réactions...qu'elles soient les bienvenues!