CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Le RSSI: un manager transverse

Thomas Jolivet
Responsable du pôle Conseil
harmonie [TECHNOLOGIE]

20/06/2013

Agenda

1. Le RSSI :un manager pas comme les autres
2. Les Interactions entre la SSI et l'organisation
3. Mobiliser les contributeurs SSI au-delà de la sensibilisation

Le RSSI : Un manager transverse

UN MANAGER PAS COMME LES AUTRES

Le rôle particulier du RSSI

Il doit gérer des risques

La SSI n'est pas une des fonctions productives de la chaine de la valeur de l'organisation, elle doit protéger le patrimoine informationnel de l'entreprise, elle apporte à priori des contraintes plus que de la valeur…

Spécialiste de la sécurité : il ne doit pas être une Cassandre(*)

Il doit développer une expertise sur des sujets pointus pour identifier les nouvelles menaces, mais il doit aussi savoir se faire comprendre et convaincre les métiers

Visionnaire: il participe aux transformations de l'entreprise

Il doit comprendre les opportunités business liées aux innovations et les accompagner

Manager: il doit mobiliser au delà de son équipe

Pour atteindre ses objectifs, il doit faire contribuer des ressources qui ne dépendent pas de lui hiérarchiquement

(*) Cassandre reçut d'Apollon le don de prédire l'avenir, mais se refusant à lui, le dieu décréta que ses prédictions ne soient pas crues.

Un manager atypique

Comme tout manager le RSSI

- Apporte une vision, propose une stratégie
- Planifie des actions
- Organise la gestion opérationnelle
- Pilote
- Contrôle

Mais:

- Sur des sujets à priori non cœur de métier
- Sur des projet de sécurité moyens et longs termes, en restant capable d'être dans du réactif… les menaces ne sont pas toutes prévisibles
- Sur des ressources humaines réparties dans l'entreprise dont la mobilisation peut être un réel challenge
- Les ROI qu'il doit défendre sont plus complexes à appréhender… (risque à ne pas faire)

Les missions spécifiques du RSSI

Les principales missions du RSSI…

1. **Gouvernance de la SSI**
2. **Sensibilisation Sécurité**
3. **Suivi des indicateurs SSI**
4. **Gestion des incidents**
5. **Veilles sur les menaces**
6. **Analyse des Risques**
7. **Prise en compte de la sécurité dans les projets**

… font de lui un manager transverse.

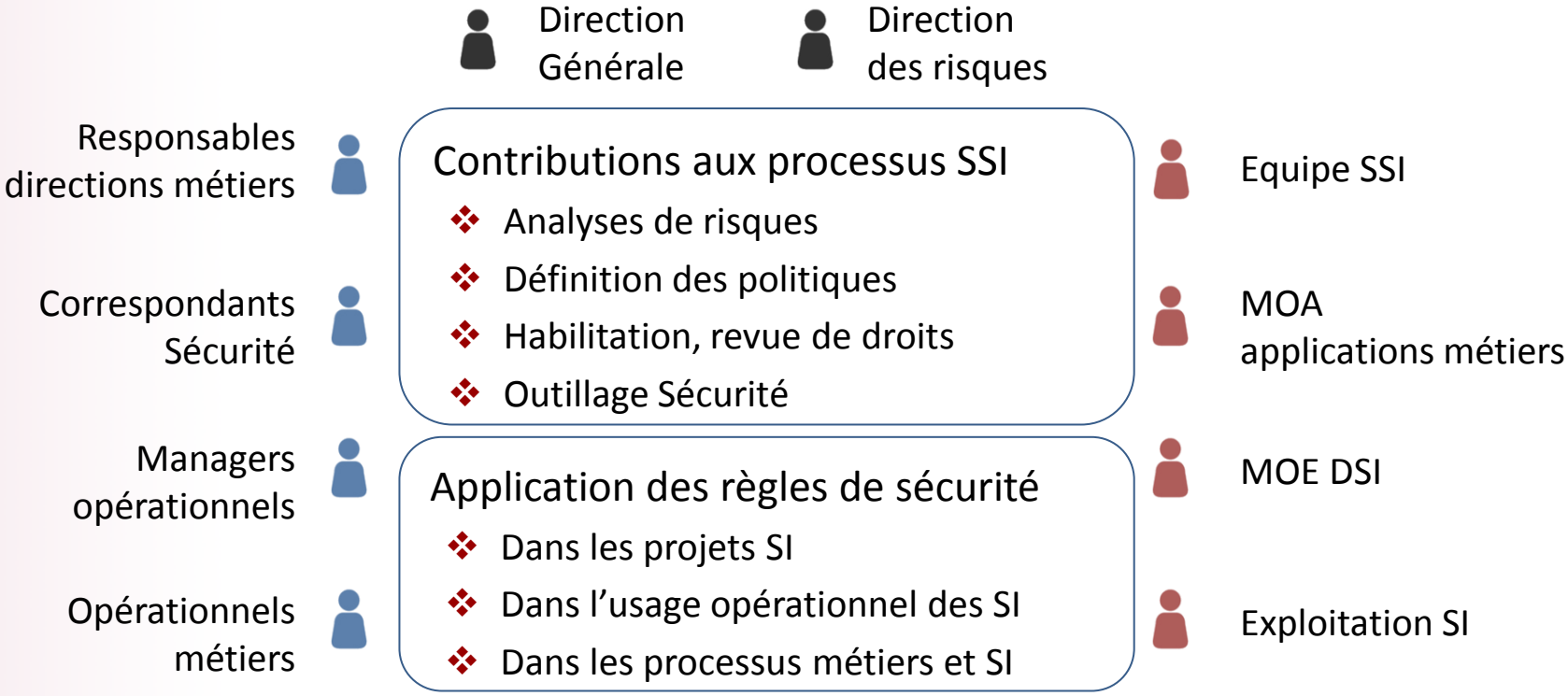
Implication et mobilisation de contributeurs appartenant à l'ensemble des directions de l'entreprise :

- ✓ **Direction Générale**
- ✓ **Direction des Risques**
- ✓ **Directions Métiers**
- ✓ **DRH**
- ✓ **DSI**

Le RSSI : Un manager transverse

LES INTERACTIONS ENTRE LA SSI ET L'ORGANISATION

Typologies de contributions à la SSI

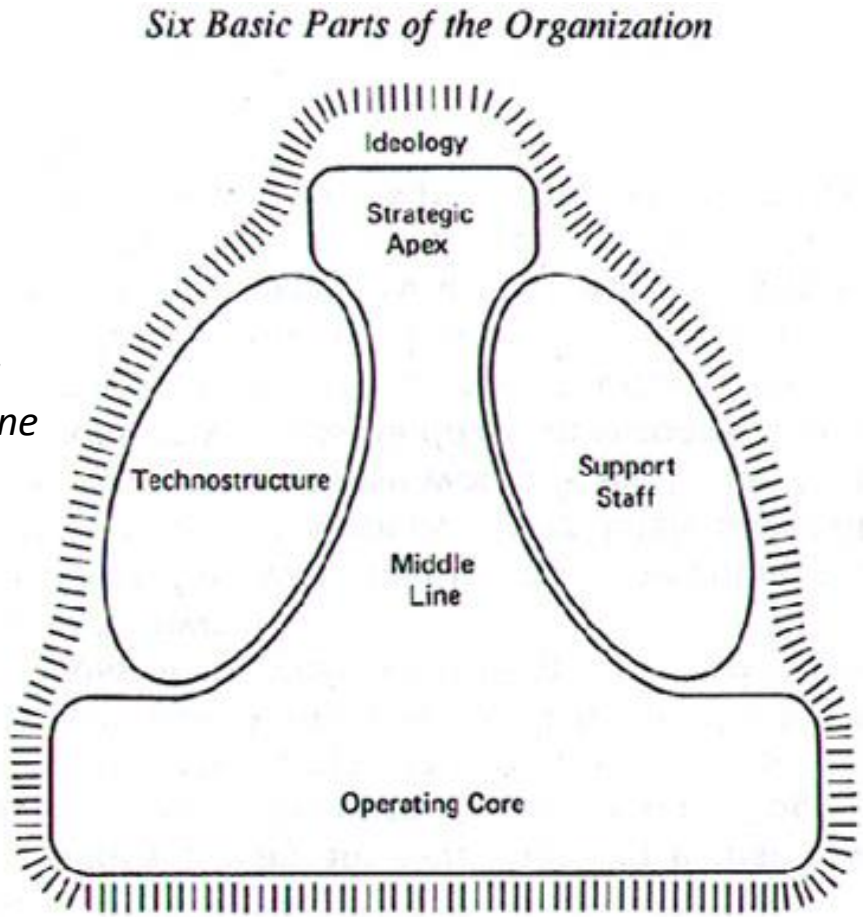


Les normes et référentiels proposent des bonnes pratiques pour organiser ces contributions, mais ne les contextualisent pas.

Les modèles d'organisation

Henry Mintzberg

Il est à l'origine d'une typologie des organisations, qui fait référence. Elle permet en particulier de bien appréhender les phénomènes de pouvoir, d'une part, et la conduite du changement, d'autre part



1979 : The Structuring of Organizations : A Synthesis of the Research - traduit en français sous le titre Structure et dynamique des organisations (Éditions d'Organisation)

Impact du modèle d'organisation

L'organisation entrepreneuriale	L'organisation mécaniste	L'organisation divisionnaire	L'organisation professionnelle	L'organisation innovatrice
				
• Activités de type PME, • Centralisation des pouvoirs	• Grandes Organisations • Grand nombre de procédures…	• Groupes avec filiales relativement autonomes	• Activités de spécialistes • Journalisme • Hopitaux • Trading • Université	• Activités de type • Projets • Consulting • Publicité • ingénierie

- **Les leviers et relais pour sensibiliser, former, mobiliser et faire appliquer les règles de sécurité vont être différents en fonction du modèle d'organisation.**
- **Les normes, les référentiels et les bonnes pratiques sont à contextualiser en fonction de la typologie de l'organisation**

Impact de la dispersion du risque

Risques concentrés sur une faible population

Exemple:
Industrie pharmaceutique

Risques répartis sur une partie de la population

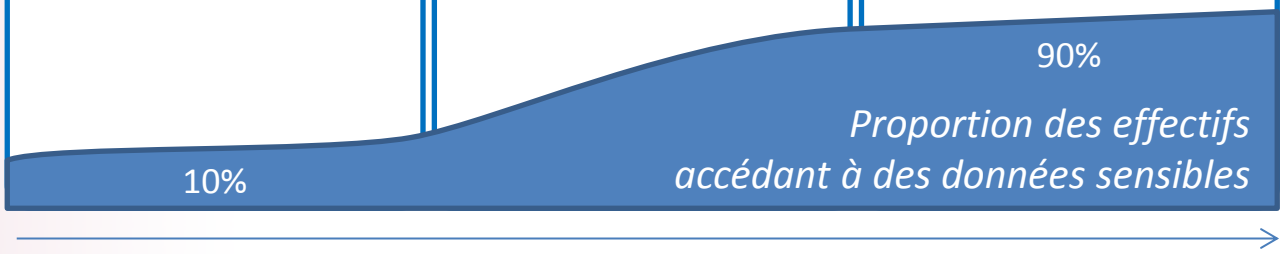
Exemple:
Service, Assurance Média

Risques forts portés par l'ensemble des effectifs

Exemple:
Banque de financement Trading

Entreprise étendue

- Ouverture des SI aux clients
- Ouvertures des SI aux partenaires



Le rôle et l'impact de la SSI n'est pas moins fort, mais les efforts ne sont pas de même nature selon la répartition des risques…

Le RSSI : Un manager transverse

MOBILISER AUTOUR DE LA SSI

La sensibilisation

- La sensibilisation est incontournable
  - Développement d'une culture du risque
  - Prise de conscience des risques et des menaces
  - Responsabilisation des personnes manipulant des données sensibles
  - Modification des comportements vis-à-vis de l'usage de l'IT
- Mais n'est pas suffisante pour mobiliser efficacement
  - Les contributeurs aux projets de sécurité
  - Les acteurs des processus SSI

Comment atteindre ces objectifs auprès de populations hétérogènes qui ont elles-mêmes des objectifs parfois à l'opposé ?

Légitimer par la doxa

- Informer sur les contraintes réglementaires
- S'appuyer sur les audits internes
  - Les injonctions ou recommandations des volets sécurité des audits
- Formaliser un SMSI sponsorisé au niveau entreprise
  - Il s'agit de rendre officiel des processus SSI, les règles et la gouvernance, en faire un processus métier comme un autre
- Introduire des aspects sécurité dans le volet RH
  - Inclure les actions SSI dans les fiches de postes, les contrats de travail, les objectifs personnels…
- Inscrire les étapes SSI dans les processus métier de l'entreprise

Les sollicitations du RSSI doivent être légitimées , cependant elle ne reçoivent pas toujours un accueil bienveillant…

Motiver les contributeurs

- Convaincre les managers des contributeurs
  - « Si ce n'est pas important pour mon chef… »
- Rendre les initiatives autours de la sécurité visibles et valorisées par la direction
- Démontrer l'intérêt pour les contributeurs de consacrer du temps à la SSI.
  - Exemple de la rédaction contributive de la PSSI

Les contributeurs doivent identifier leur intérêt propre à s'impliquer

Démontrer la valeur apportée

- Continuité
  - Faire de la sécurité : c'est un des moyens permettant de garantir la continuité de l'activité opérationnelle
- Assurance
  - Consacrer du temps et des budgets aux sujets SSI c'est souscrire une assurance
- Création de valeur
  - SSI et création de valeur ne sont pas des notions systématiquement contradictoires : CLOUD, BYOD, Mobilité, ouverture du SI aux partenaires, aux clients…

Le RSSI n'est pas quelqu'un qui dit toujours non, mais qui doit maîtriser

Conclusion

- Vos retours d'expérience à partager ?