Règle n° 2 : Nommer un responsable de la sécurité numérique et mettre en place une gouvernance

Le développement croissant de la cybercriminalité, des menaces pour les ressources d'informations critiques de l'entreprise, tout comme celles de la règlementation, commande aux conseils d'administration et aux dirigeants de s'engager pleinement en faveur de la sécurité numérique dans leur gouvernance.

En tant que ressource critique, l'information doit être traitée comme tout autre actif essentiel au succès de l'entreprise. Ainsi, afin de permettre la réalisation de ses objectifs, elle doit mettre en place une stratégie de gouvernance cybersécurité,

L'information étant devenue essentielle aux activités métiers et support, la sécurité numérique affecte tous les aspects de l'entreprise et il est recommandé de :

- **Nommer un responsable de la sécurité numérique.** Le dirigeant d'entreprise est de facto responsable de la sécurité mais la désignation d'un responsable de la sécurité de l'information est un prérequis à une gouvernance efficace. Il est de bonne pratique qu'il :
  - Soit rattaché à la direction, des systèmes d'information ou des risques, et dispose de la capacité de remonter des alertes à la direction générale
  - Dispose des moyens et de l'autorité nécessaires à la réalisation de sa mission
  - Se voit attribuer un budget pluriannuel sanctuarisé par la Direction Générale
  - Définisse et maintienne une politique de sécurité de l'information de l'entreprise
  - Réalise un reporting en comité de direction à minima une fois par an pour faire le bilan des risques, des incidents, des projets en cours et des budgets requis
- **Mettre en place un comité sécurité numérique impliquant tous les acteurs pertinents de l'entreprise (Dirigeant, DAF, DSI, RSSI, DO, DRH, DJ…) :**
  - Il est animé par le responsable de la sécurité de l'information et permet de créer un canal de communication efficace pour les orientations de la direction
  - Il permet d'assurer l'alignement stratégique en matière de cybersécurité
  - Il est l'outil de la conduite du changement et de la promotion de la culture cybersécurité

En toute hypothèse, il est indispensable que la direction comprenne la criticité de l'information pour l'entreprise et s'implique directement dans la gouvernance sécurité.

Faits

77% des entreprises déclarent avoir une forte dépendance au système d'information

62% des entreprises ont désigné un RSSI

46% des RSSI sont rattachés à la DSI, 27% à la Direction générale, 8% à la DAF, 3% à la Direction des risques

64% des entreprises ont formalisé leur politique sécurité de l'information

Source: Rapport du CLUSIF sur les Menaces informatiques et les pratiques de sécurité en France - 2014

Résultats attendus

Alignement la gouvernance sécurité sur la stratégie d'entreprise

Identification et gestion adaptée des risques cybersécurité

Développement d'un programme et des projets cybersécurité pour réduire et gérer les menaces cyber

Intégration de la cybersécurité dans les processus métiers et support de l'entreprise

Reporting annuel au comité de direction

Liens

www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_informatique_anssi.pdf

http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d