OPUS 6

APSSIS

GUIDE CYBER RÉSILIENCE

GOUVERNANCE
LE GUIDE DU RSSI INTERGALACTIQUE

Par Cédric CARTAU

SOMMAIRE

CYBER RÉSILIENCE

0.6 LE GUIDE DU RSSI INTERGALACTIQUE

SOMMAIRE

CYBER RÉSILIENCE

0.6

SOMMAIRE

CYBER RÉSILIENCE

0.6

SOMMAIRE

CYBER RÉSILIENCE

0.6

L'AUTEUR

Cédric CARTAU est RSSI et DPO du CHU de NANTES et du GHT44. Il est vice-président de l'APSSIS et enseigne à l'EHESP, à l'ESIEA et au CNEH. Il est également auteur de plusieurs ouvrages chez Eyrolles ou aux Presses de l'EHESP, sa dernière publication étant « La sécurité du système d'information des établissements de santé », en 2018.

cedric@cartau.net

L'auteur et l'APSSIS remercient ces contributeurs d'avoir accepté le difficile exercice de présenter une approche métier sur une question aussi complexe que la gouvernance.

1. INTRODUCTION

Le profil de poste d'un RSSI - ce qu'il fait, ce qu'il ne fait pas - est un sujet de discussions entre les RSSI eux-mêmes mais aussi avec les professions qui ont affaire aux RSSI : Directions Générales, DSI, chefs de projet, etc.

Nous constatons également que les RSSI récemment nommés expriment souvent des difficultés sur une question somme toute basique : par quoi dois-je commencer en arrivant dans ce poste, qui est, il faut le dire, un peu bizarre par certains moments ?!

Par quoi commencer ? Comment se positionner ? Quelle limite de son action ? Quelle partie non négociable de son périmètre de décision ? Quels outils méthodologiques ? Quel type de pouvoir (soft ou moins soft) ? Autant de questions pour lesquelles il n'existe que peu de publications ou d'ouvrages de fond, la plupart des productions existantes se focalisant sur la technique ou les outils (logiciels ou matériels).

Cette publication s'inscrit dans la suite des précédents guides de cyber résilience (Tome 1 : les mots de passe ; Tome 2 : les cyberattaques ; Tome 3 : les habilitations d'accès aux données métier, Tome 4 : la protection du Cloud ; Tome 5 : les indicateurs), publiés avec le précieux concours de l'APSSIS avec l'ambition de constituer un corpus de référence sur les questions relatives à la sécurité du SI.

Comme pour chaque guide, les contributions en annexe constituent un complément très riche, des points de vue de professionnels du secteur chacun dans sa spécialité.

Et comme toujours, les remarques, suggestions d'amélioration sont à envoyer directement à l'auteur pour être prises en compte dans les prochaines versions.

Bonne lecture.

2. LE RSSI, QUELLES MISSIONS

2.1 Définition du métier

Parler du métier de RSSI c'est d'abord le définir, et pour cela la meilleure source reste sans discussion possible l'annuaire des métiers SI du CIGREF, qui est régulièrement mis à jour depuis 1991.

Dans sa version de 2021 (voir Annexe «14.14 Fiches métier SSI» pour le lien), l'annuaire définit clairement trois métiers autour de la sécurité des SI :

• l'expert en cyber sécurité (eCS) ; certains le nomment « Correspondant en sécurité SI », ou expert en sécurité SI (nous conserverons la dénomination du CIGREF) ;
• l'auditeur SSI (aSSI) ;
• le responsable de la sécurité des SI, ou RSSI ;

Il y a souvent confusion entre l'eCS et le RSSI et il n'est pas rare de croiser des experts en Cyber Sécurité qui se présentent comme des RSSI. Parmi les différences notables (il y en a pas mal), le eCS est souvent dédié à des actions techniques (Pentest, audit de vulnérabilité, etc.) et n'est pas supposé aborder le volet métier (MOA) de la SSI : l'assistance à la rédaction des procédures dégradées métiers n'est pas dans son périmètre, pas plus que les appréciations des risques avec les MOA ni la négociation des budgets SSI avec la Direction Générale. A contrario, un RSSI - surtout dans une structure de taille conséquente - n'est pas en situation de manipuler des outils techniques complexes, et perd d'ailleurs rapidement la technicité nécessaire du fait des autres tâches qui absorbent son quotidien.

Liens hiérarchiques ou fonctionnels entre eCS et RSSI

Il n'y a pas nécessairement de liens hiérarchiques entre ces deux fonctions : le RSSI peut parfaitement se trouver hors de la DSI (c'est mieux) et le eCS en plein dedans, aucun souci. Par contre, les liens fonctionnels sont très forts, chacun alimentant l'autre de ses contraintes et de ses feedbacks.

On retiendra donc comme définition des missions du RSSI celle du CIGREF qui fait foi, à savoir :

« Sa mission première est de s'assurer et garantir la bonne application de la politique de sécurité du SI. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il préconise toute décision d'intervention sur les systèmes d'information, dans leur globalité, de son périmètre pour préserver l'intégrité et la continuité du SI. »

La version de la FPH

Le répertoire des métiers de la Fonction Publique Hospitalière donne une version quasi identique du métier de RSSI.

2.2 Les missions du RSSI : ce que cela est, ce que cela n'est pas

En 2019, j'ai publié dans DSIH Magazine une série d'articles sur ce que n'est pas un DPO (voir annexe «16. Annexe 5 : ce que le DPO n'est pas»). Ce point déroute pas mal de DPO, et encore plus de RSSI (qui sont souvent issus de la technique) et qui, on le constate, ont du mal à « faire leur deuil » de leur capacité à infléchir l'organisation. Le sujet est identique entre les deux métiers : il s'agit de la différence entre l'opérationnel et le conseil.

Un expert technique (eCS, ingénieur réseau, développeur, etc.) utilise les outils dont il dispose pour configurer un LAN, développer un nouvel écran, patcher des machines, etc. Bref, il agit. Et sauf à ce qu'il fasse des bêtises, personne n'a à lui dire comment faire son travail dans son volet MOE (sa MOA lui impose bien entendu les objectifs mais pas la façon d'y arriver).

Le métier de RSSI a ceci de bizarre qu'il ne s'exerce qu'en conseil, alerte et audit. Il conseille une MOA sur des points relevant de la SSI, mais en dernier recours la MOA décide ou pas de suivre ces conseils, car la MOA est propriétaire de ses propres risques métiers.

MOA et risques

La MOA est propriétaire de ses risques métiers, le RSSI n'est en fait Responsable d'aucun risque et dans les pays anglo-saxons, il se nomme « Officier Sécurité IT » ou CISO pour Chief Information Security Officer.

Même si, stricto sensu, le RSSI ne devrait pas procéder lui-même à des appréciations des risques (AR) (c'est à la MOA de le faire), dans les faits ce sujet est assez technique et c'est une des missions du RSSI, surtout quand on parle de risques systémiques qui touchent toute l'organisation et pas simplement une MOA précise. Mais que cela soit clair : en déroulant une AR, un RSSI n'est que le factotum d'une MOA (qui devrait dérouler elle-même cette AR mais n'a pas forcément les compétences pour le faire), mais une fois cette AR déroulée, la MOA seule valide cette AR, décide des risques qu'elle réduit et tient compte, ou non, de l'avis et des alertes du RSSI.

Risques et voitures

Je vous alerte sur le fait qu'il est dangereux et illégal de ne pas mettre sa ceinture de sécurité quand on prend le volant. Mais c'est vous qui voyez : votre voiture, votre décision, votre responsabilité juridique, votre vie.

Par contre, corollaire du point précédent, personne n'a à imposer au RSSI les conseils et alertes qu'il doit ou pas faire remonter. Le RGPD est au moins clair sur ce point, stipulant que le DPO ne reçoit pas d'instructions dans l'exercice de sa mission (art 38 et 39), mais il en va de même pour le RSSI - sinon le conseil pourrait être biaisé. C'est d'ailleurs l'un des rares éléments qui pourrait engager la responsabilité juridique du RSSI (comme celle du DPO), quand il n'a pas exercé son devoir de conseil et d'alerte, qui doit donc logiquement être non-entravé. Il appartient au RSSI d'alerter, de conseiller, de bien veiller à ce que la MOA ait compris ses conseils

et alertes (et cela peut être très complexe dans certains cas) mais le reste du film ne le concerne pas.

De la même manière, la fonction d'audit du RSSI ne souffre d'aucune restriction (il doit pouvoir auditer ce qu'il veut quand il veut), et les recommandations issues de ses audits suivent le même processus que les conseils et alertes ci-dessus.

Cela paraît étrange aux nouveaux venus dans la profession, mais les situations suivantes (qui ne sont là qu'à titre d'exemples pour illustrer le propos de façon quasi caricaturale) ne sont en aucun cas une anomalie :

• une MOA qui refuse un audit du RSSI ;
• une MOA qui reçoit une AR du RSSI mais décide de ne pas en tenir compte ;
• une MOA qui a bien compris les alertes du RSSI sur un dysfonctionnement détecté mais qui décide de passer outre ;
• une MOA qui réalise elle-même ses AR SSI sans en référer à son RSSI, ni sur la méthode ni sur le résultat ;
Si une telle situation devait se produire, le RSSI doit simplement tracer les échanges, rien de plus.

Par contre, les situations suivantes sont des anomalies :

• une MOA qui demande au RSSI de modifier son AR au motif que cela ne lui plait pas ;
• une MOA qui demande au RSSI d'endosser un risque résiduel ;

Le RSSI doit absolument refuser de rentrer dans ces pièges, aucune négociation ne devant être possible.

Quand tout se passe bien (ce qui est le plus souvent le cas), la répartition de conseil / alerte et de propriété des risques est claire, chacun (RSSI et MOA) sait où s'arrête la mission de l'autre et où commence sa propre responsabilité. Ce point nécessite toutefois des rappels réguliers de la part du RSSI.

De bon ton

Il est de bon ton, pour un RSSI, de rappeler à une MOA qu'il n'est qu'en conseil et alerte. D'une part pour mettre cette MOA devant ses responsabilités, mais aussi pour lui dire que l'avis du RSSI n'est pas suspensif. D'expérience, cela facilite le relationnel.

Dans les rares cas (ils sont vraiment rares) où la discussion peut devenir compliquée, la seule attitude du RSSI doit être de tracer les échanges, et de s'en tenir là, tout en restant courtois. Une MOA qui refuse de tenir compte des alertes ? Courrier ou mail interne, horodaté et avec accusé de réception. Une alerte sur un risque d'obsolescence auprès de la DSI ou de la DG qui n'est pas suivie d'un plan d'action ? Une présentation sous forme de slides, horodatée avec copie interne. Ne pas oublier que le RSSI peut être mis en cause pour défaut de conseil, et c'est bien cela qui va être examiné à la loupe en cas de dysfonctionnement grave du SI.

L'impression PDF pour salut

Je conseille fortement de conserver les mails litigieux, non pas dans le système de messagerie, mais en les exportant sous format PDF dans un répertoire spécial, dans l'espace de fichiers du RSSI, avec un système d'horodatage de type date à l'envers dans le nom du fichier.

Dans l'immense majorité des cas, le relationnel se passe bien, il faut tout de même le signaler. A titre personnel, en plus de 12 années de poste, sur des centaines de sollicitations et de dossiers instruits, le

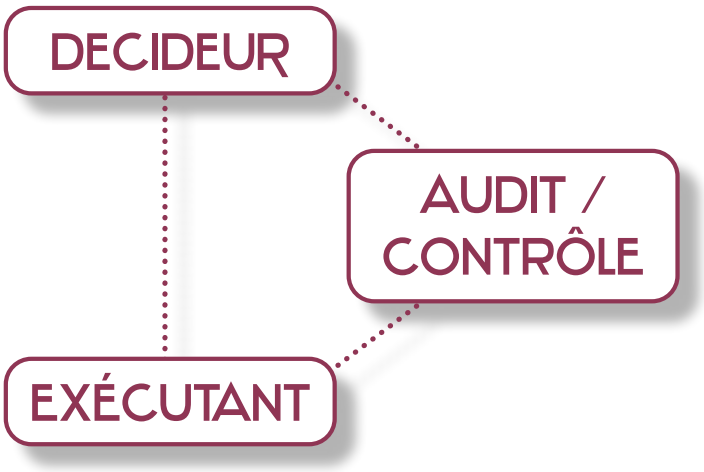
nombre de dossiers vraiment compliqués se compte sur les doigts d'une seule main.

Les amis et les ennemis

Les amis coûtent cher au RSSI (ils lui demandent toujours des services, des dérogations, etc.) mais les ennemis lui coûtent encore plus cher. Rester professionnel, courtois, bien expliquer le périmètre du poste et la limite du rôle de conseil et d'alerte. Surtout, rester en bons termes avec l'ensemble des interlocuteurs.

2.3 Rattachement hiérarchique

Partant de là, il est clair que le RSSI ne peut en aucun cas dépendre hiérarchiquement du DSI. J'ai participé à des dizaines de débats sur la question, je n'argumente même plus. Le principe de base des organisations modernes, et ce depuis au moins l'affaire Enron, est la séparation entre ceux qui décident, ceux qui exécutent et ceux qui contrôlent (le scandale Enron est entre autres imputable à la collusion entre la fonction de décision et la fonction de contrôle).



De la même manière que les Commissaires aux Comptes (CAC) sont strictement indépendants de l'entreprise qu'ils contrôlent (ils sont certes liés par un marché mais engagent leur responsabilité civile et pénale en cas de manquement avéré à leurs missions, d'où leur indépendance), toute fonction de contrôle interne (RSSI et bien évidemment DPO) ne peut pas hiérarchiquement dépendre de l'entité qu'il contrôle. Au moins pour le DPO c'est clair (art 38 et 39, toujours), pour le RSSI cela commence à faire son chemin, même si certains DSI font de la résistance.

La mauvaise foi caractérisée

Lors d'une discussion avec un DSI dont je tairai le nom, ce dernier voulait garder le RSSI « à sa botte » et n'avait strictement aucun argument à part que le rattachement du RSSI est de la décision du DG (décision qu'il se chargeait d'orienter dans le sens qui lui convenait cela va sans dire). Et moi de lui faire remarquer le parallèle avec le DPO, les CAC (qui sont régis par une réglementation à laquelle le DG doit se plier) mais il n'en démordait pas, cela relevait de la décision du DG. Il n'y a pas pire sourd que celui qui ne veut rien entendre.

Globalement, rien qu'en observant la position hiérarchique du RSSI, il est possible d'en déduire la maturité de l'entreprise au regard de la problématique SSI :

• cas du « paper RSSI » : très courant, l'entreprise a juste « bombardé » RSSI celui qui s'occupe de l'antivirus ou des règles du pare-feu ; non seulement il y a collision entre la fonction de MOA (le RSSI est MOA de la SSI) et de MOE (l'agent en question est en exécution), ce qui est interdit, mais en plus on voit mal comment un informaticien déjà bien chargé pourrait en sus assumer une fonction qui réclame un large plein temps ;
• cas du RSSI rattaché à la DSI : on retrouve la collision MOA / MOE, en plus de l'absence d'indépendance, pourtant indispensable ; l'argument selon lequel le RSSI doit être « dans les équipes DSI pour mieux collaborer » ne tient pas 2 minutes (depuis quand une MOA doit-elle être intégrée au sein de sa MOE ? Heureusement que cela n'est jamais le cas, sinon le BTP n'aurait jamais vu le jour) ; dans ces cas, on n'a pas affaire à un RSSI mais à un eCS ;
• cas du RSSI en MOA et détaché de la DSI, ce qui est le cas le plus favorable pour les raisons susnommées.

Dans le dernier cas, où rattacher le RSSI ? Il y a plusieurs solutions, qui sont « personne-dépendante », aucune n'est mauvaise en soi et tout dépend du contexte global. On peut citer entre autres :
• un rattachement au N+1 du DSI (ils auront le même chef) ;
• un rattachement à la Direction Qualité (la SSI n'est jamais que de la Qualité appliquée au SI) ;
• un rattachement à la Direction de la sécurité des biens et des personnes, au motif que sécurité physique et logique ont des synergies ;
• un rattachement DG (compliqué dans les gros CHU), ou DG adjoint voire Secrétaire Général (excellente solution dans les CHU) ;
• un rattachement à la Direction de la Conformité s'il y en a une ;

Globalement, de plus en plus de publications, d'instructions voire de textes opposables tendent à détacher le RSSI de la DSI, c'est donc clairement le sens de l'Histoire.

2.4 RSSI, quelle maturité

Globalement, on peut classer les RSSI selon l'échelle de maturité suivante. L'exercice est redoutable, et il est surtout frustrant pour un RSSI qui est au niveau 4 d'expliquer à une organisation qui ne connaît que le niveau 1 qu'il en existe 4 autres !

2.4.1 Niveau 1 : un « paper RSSI »

No comment.

2.4.2 Niveau 2 : RSSI technique au sein d'une DSI

C'est toujours mieux que rien, mais ce n'est pas un RSSI.

2.4.3 Niveau 3 : RSSI fonctionnel, sorti d'une DSI

Une bonne part des entreprises n'ont pas atteint ce cap, même si comme nous l'avons vu cela a tendance à devenir une obligation réglementaire.

2.4.4 Niveau 4 : RSSI processus

Il veille à la mise en place de processus (homologation des projets, contrôle des habilitations) et réalise des contrôles. Peu d'hôpitaux ont franchi cette étape, qui est consubstantielle à une certification ISO.

2.4.5 Niveau 5 : RSSI processus second niveau

Il met en place des processus, désigne des propriétaires, les amène à réaliser eux-mêmes leurs contrôles ; dans ce contexte, le RSSI est en contrôle des processus de contrôle. A notre connaissance, aucun hôpital n'a atteint ce niveau en 2022.

3. LA GOUVERNANCE SSI

Une fois que l'on sait ce qu'est ou n'est pas un RSSI, la question est maintenant de savoir comment ce dernier anime, au sein d'un établissement de taille variable, la démarche globale, et dans quelle organisation il s'inscrit. Il y a deux types d'instances : celles qu'il pilote et anime, et celles auxquelles il participe.

3.1 Les instances pilotées par le RSSI

Il est pratique de se caler sur le découpage habituel : stratégique / tactique / opérationnel.

3.1.1 L'instance stratégique

Il s'agit d'une instance qui a pour objectif que la Direction Générale et le RSSI échangent, idéalement deux fois par an.

Il s'agira d'évoquer :

• le contexte global cyber, à la fois au niveau mondial et à l'échelon national et sectoriel santé ; les incidents récents sont un excellent point d'entrée ;
• les grandes orientations cyber internes, en lien avec les projets nationaux ;
• les projets cyber internes, au niveau macroscopique ; par exemple le lancement d'un chantier d'étude d'une assurance cyber risque relève de cette instance de pilotage ;
• les difficultés rencontrées, à la fois organisationnelles et de moyens (humains ou financiers) ; l'arbitrage sur les grandes masses budgétaires se passe là ;
• les risques résiduels non pris en compte ; ce point est absolument majeur car au final c'est la Direction Générale qui porte le risque résiduel cyber, pour autant qu'elle en ait été mise au courant (toujours ce rôle de conseil et d'alerte) ;

Rapport annuel cyber, tellement vieille école mais tellement utile

A notre connaissance aucun texte ne l'impose, mais produire chaque année un rapport global sur l'état cyber de son établissement avec les éléments susnommés dans le point DG, permet d'être utilisé comme base de discussion...et laisse une trace tangible.

La question de savoir si ce point DG-RSSI doit ou non être fait en présence du DSI fait débat, il y a des avantages et des inconvénients aux deux solutions.

Les interventions ponctuelles

Dans un monde parfait, le RSSI doit pouvoir intervenir ponctuellement, à sa demande ou sur sollicitation, en réunion de direction (établissement ou GHT), quand l'actualité ou les projets le nécessitent.

De façon générale, une des valeurs ajoutées d'un RSSI est son « agilité organisationnelle » : il doit pouvoir intervenir dans différentes instances (réunions de Direction, CME, réunions de pôle, etc.) et tenir un discours

adapté à son auditoire : on ne parle pas de chiffrement homomorphe à un Directeur Général ou un Président de CME !

3.1.2 L'instance tactique

Il s'agit plutôt d'une instance avec la DSI qui se tient à minima tous les trimestres (tous les mois c'est mieux) et qui a pour objectifs principaux :

- d'arbitrer les projets techniques SSI ;
- de prioriser les projets SSI versus les autres projets de la DSI ;
- de communiquer les sujets issus des instances nationales (ANSSI, ANS, DGOS, etc.) auprès des équipes lorsque cela traite de points techniques ;

A cette instance sont aussi remontés les indicateurs issus d'une démarche ISO 27001 (c'est une obligation) en rapport avec les objectifs de sécurité : cela peut être un taux de disponibilité cible de la plateforme technique, un taux de formation à la SSI des agents de la DSI, etc.

Des indicateurs de pilotage

Personnellement, j'aime bien communiquer aux équipes des indicateurs qui, sans être à proprement parler des objectifs de SSI, donnent une idée de l'activité SSI globale : nombre de sujets en cours de traitement / sujets déjà traités, état d'avancement annuel des contrôles, etc.

3.1.3 L'instance opérationnelle

Il s'agit de réunions avec les équipes techniques de la DSI (essentiellement les ingénieurs réseaux, système, exploitation, éventuellement le responsable IAM / AD s'il y en a un). Elles se tiennent à minima une fois par mois et ont pour objectifs :

- de suivre l'état d'avancement des projets et actions recensés dans un DSA (Dossier de Suivi d'Action) ;
- de faire des arbitrages ;
- de préciser les besoins du RSSI et les attentes des équipes MOE sur d'éventuelles précisions ;
- d'évoquer l'actualité, les nouvelles menaces, etc.

Variantes

Ces trois instances peuvent porter différents noms ou acronymes selon les établissements : comité stratégique, comité de pilotage, etc. L'important est de bien trouver ces trois strates, et surtout d'avoir un discours adapté à l'instance : à nouveau, on ne parle pas de chiffrement asymétrique dans une instance stratégique de GHT !

3.2 Les instances auxquelles participe le RSSI

Stricto sensu, le RSSI est susceptible d'intervenir à peu près partout, soit sur demande de l'instance en question, soit à sa propre demande en cas d'actualité (nouvelle

réglementation, nouvel incident, instruction ministérielle impactant l'ensemble des équipes, etc.).

Nous pouvons citer, sans que cela soit exhaustif :

• pour ce qui est de la gouvernance d'établissement : réunion de Direction, CME, CTE, Directoire, Conseil de Surveillance, etc. ;
• pour ce qui est des directions fonctionnelles : réunions de service, réunions Qualité, groupe de travail thématique (acheteur, Recherche / Innovation), etc. ;
• bien évidemment, toute intervention dans les pôles médicaux et médico-techniques (Laboratoires, Imagerie, Pharmacie).

Tracer les interventions

Un document de présentation, un ordre du jour, une invitation même électronique doivent être conservées et archivées par le RSSI car ce sont des éléments de preuves exigibles par l'ISO 27001 dans le processus COMMUNICATION.
Le petit conseil : préfixer chaque document par la date sous format AAAA-MM-JJ, cela permet de retrouver facilement l'historique classé par date.

3.3 Les rôles et responsabilités des directions fonctionnelles

Les rôles et responsabilités des pôles administratifs, médicaux et médico-techniques sont :

• de définir leur niveau de besoin face au risque cyber
• d'écrire les procédures dégradées métier ; curieusement on entend souvent dire que c'est à la DSI de les rédiger, et c'est totalement faux ;
• de piloter les exercices cyber, selon un rythme, un périmètre à définir conjointement avec le RSSI et d'autres groupes de travail dans l'établissement ;

La question des risques résiduels est absolument majeure : il faut les identifier et les afficher, à la manière d'un catalogue de services dans lequel est formalisé le point au-delà duquel la MOA est incapable de garantir quoique ce soit. Par exemple, les infrastructures Datacenter peuvent assurer un certain niveau de redondance, mais sans tenir compte du scénario d'une panne électrique totale en plus d'une panne informatique : dans ce cas précis, la limite du PCA-PRA est de considérer que l'alimentation électrique est assurée, le risque résiduel d'un PCA-PRA est donc celui de l'absence de panne électrique concomitante.

Le SLA de la DSI, ses limites

Le Service Level Agreement de la DSI (ce à quoi elle s'engage et qu'elle affiche) porte en grande partie sur la disponibilité du SI, aussi bien matérielle que logicielle. Il s'agit ni plus ni moins de dire que la DSI s'engage à ce que les pannes en heures ouvrables soient résolues dans 80 % des cas en 2h, (4h en heures non ouvrables dans l'exemple). Les MOA doivent tenir compte de ce SLA pour calculer le leur, mettre en place les procédures dégradées adéquates et afficher elles-mêmes leur SLA.

CYBERSÉCURITÉ : L'ENJEU DE LA GOUVERNANCE

Par Xavier JUNG, Manager chez WELIOM

Approche métier : Point de vue de WELIOM

Nous sommes régulièrement sollicités par nos Clients pour les accompagner dans la définition et la mise en œuvre de systèmes de gouvernance de la sécurité des Systèmes d'Information. Il s'agit de définir et de déployer un système de management de la sécurité adapté, alimenté par l'état de l'art mais aussi par les exigences et les contrôles particuliers aux structures de santé, OSE ou non. Pour être efficiente, il est admis que cette gouvernance doit être positionnée au plus haut niveau de l'organisation (Direction générale, Secrétariat général…) et doit disposer de l'adhésion et de l'appui de celle-ci. Le RSSI étant avant toute chose un « conseiller », sans pouvoir direct sur les organisations, ses recommandations ne peuvent être suivies d'effets sur la structure que s'il dispose de suffisamment de crédibilité institutionnelle. La gouvernance de la SSI se doit d'embarquer l'ensemble des parties prenantes (Directions fonctionnelles, Directions métiers, DSI, …), et être pilotée par un véritable chef d'orchestre, disposant des bonnes compétences, d'une vision stratégique, d'une trajectoire et de budgets directs ou indirects adaptés.

1. Une comitologie à 2 niveaux

Qui dit gouvernance dit pilotage. La définition et la mise en œuvre d'une comitologie en est un prérequis. Principalement animées par le RSSI, les instances de pilotage sont structurantes et permettent de créer du lien avec les différentes parties prenantes de la sécurité. Elles sont généralement de plusieurs natures :

• Stratégique

En présence des membres décisionnaires, les enjeux sont de valider et suivre une feuille de route, des orientations stratégiques, des objectifs de sécurité et des moyens pour les atteindre.

• Opérationnelle

Plus proche du terrain, en présence des maîtrises d'œuvres techniques ou métiers, le RSSI conseille, contrôle, alerte sur des projets et trouve des compromis entre les besoins fonctionnels des métiers et des objectifs de sécurité.

Pour être efficient, le pilotage d'une instance se doit d'être structuré : calendrier de réunions avec fréquence régulière et adaptée, liste à jour des participants, ordre du jour et compte-rendu systématiques, plan d'actions et suivi d'indicateurs. Ces instances doivent être le lieu d'arbitrages, de prises de décisions et de partage d'informations en cohérence avec leur nature et objectif (stratégique vs opérationnelle).

2. Un responsable avec une feuille de route validée

Cette gouvernance, à la tête du « projet sécurité », doit être accompagnée de la désignation d'un (ou d'une) chef d'orchestre qui aura pour mission de piloter « l'activité sécurité » en transversalité. Plutôt technique ou organisationnel mon RSSI ? Pour répondre à cette question, il faut repartir du rôle même du RSSI. Sa mission principale est de mettre en place et d'assurer le bon déroulement d'un Système de Management de la Sécurité de l'Information (SMSI). Ce système est basé sur une démarche d'amélioration continue appliquée à la sécurité du SI : mise en place d'une gouvernance, analyses de risques, suivi de plans d'actions, suivi d'indicateurs, actions correctives… Il requiert donc un pilote, à plein temps, qui n'aura pas la bande passante pour garder les mains dans le moteur. Fini le paramétrage des matrices de flux du Firewall ou la configuration de l'antivirus, même si ces connaissances « techniques » seront toujours très utiles au RSSI ! Ce pilote, délégué de l'AQSSI (Autorité Qualifiée pour la Sécurité des SI), aura pour mission d'auditer et de conseiller les métiers, y compris la DSI. Pour cela, nul besoin d'être un expert technique, même si un socle de connaissances de base reste essentiel.

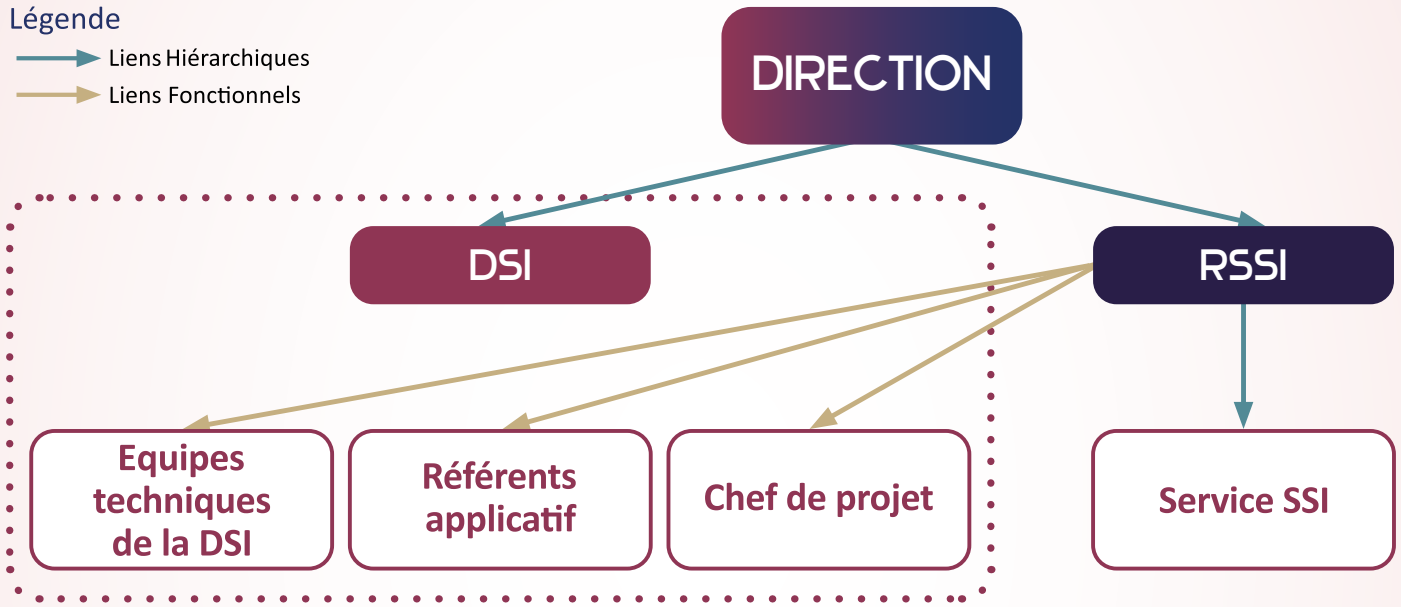
Le positionnement du RSSI est un sujet non encore abouti dans le secteur de la santé. Dans les faits, le RSSI est encore souvent rattaché à la Direction des Systèmes d'Information. Afin de pouvoir assurer son rôle de contrôle et de conseil de façon indépendante, son positionnement hors de la DSI est préférable. Directement rattaché à la Direction Générale, à la DGA, ou à la Direction de la Qualité, il pourra pleinement exercer son rôle, en transversalité, et impacter les principaux processus métiers. Par ce positionnement et grâce à la comitologie détaillée précédemment, le RSSI devient le maillon faisant le lien entre la vision stratégique et réglementaire de la SSI et sa mise en œuvre opérationnelle, par des politiques, des procédures, des plans d'actions.

3. Des ressources, du maillage

L'une des principales difficultés rencontrées dans les structures de grande taille est de réussir à faire parvenir son message à l'oreille de tous… Ainsi, on comprend rapidement que le RSSI va avoir besoin d'alliés, de relais, de porte-paroles pour diffuser ses conseils et les bonnes pratiques de sécurité. Il devra pouvoir s'appuyer sur des ressources ayant pour rôle, entre autres, de porter la bonne parole auprès des équipes, de participer au maintien en conditions opérationnelles de sécurité des systèmes et des processus, d'en intégrer de nouveaux dans le respect des bonnes pratiques, de contribuer à la réalisation d'audits internes… Ce maillage permettra un contact régulier avec les utilisateurs, au plus proche de leurs usages et du terrain.

A maturité, on peut imaginer un service sécurité de l'information composé de profils hiérarchiquement rattachés au RSSI (RSSI adjoint, auditeurs SSI, analystes SOC, administrateurs dédiés aux systèmes de sécurité ou aux identités) et travaillant avec les chefs de projets métiers et les équipes techniques de la DSI (voir schéma ci-dessous).

Exemple d'organigramme SSI (Liens Fonctionnels et Hiérarchiques)



4. Une stratégie évolutive

Intègre-t-on « de la sécurité à tous les niveaux requis du SDSI », ou construit-on un Schéma Directeur de la SSI (SDSSI), en transversalité de tous les processus métiers, y compris le processus SI ? Plus l'on converge vers des modèles certifiants, plus le SDSSI, basé sur un SMSI, va devenir incontournable.

On peut imaginer un SDSSI aborder les mêmes strates que le SDSI et lui appliquer les mêmes procédés :

- Réaliser un audit sur toutes les strates concernées, poser un diagnostic
- Définir sa cible, la trajectoire de mise en oeuvre à 3 ans et la chiffrer en ressources humaines et financières.

Cette trajectoire peut alors couvrir tous les maillons composant la sécurité :

- La règlementation, primordiale car elle donne souvent les grandes orientations.
- La stratégie SSI, adaptée aux enjeux stratégiques de la structure.
- L'organisation de l'équipe SSI, avec des liens hiérarchiques ou fonctionnels avec les différents acteurs, l'outillage de l'équipe SSI ou l'usage partagé de celui de la DSI.
- La communication entre les différentes

parties prenantes. Avoir un plan de communication permet de transférer le bon message aux bonnes personnes via le bon canal (indispensable quand tout va bien mais surtout en temps de crise).

• La sensibilisation / formation de tous les professionnels à la SSI, le pilotage de ce plan de sensibilisation et la centralisation d'éléments de preuves et d'évaluations de ces actions.

L'intérêt d'une telle démarche de construction d'un plan stratégique dédié à la SSI est similaire à la démarche réalisée lors de l'élaboration d'un schéma directeur SI : donner une vision, élaborer un plan, pouvoir communiquer aux instances décisionnaires, définir au plus juste un budget annuel et être en capacité de le défendre, en présentant une vision d'ensemble priorisée, répondant aux enjeux à court et moyen termes.

5. Un budget ? Quel budget ?

Puisque l'on évoque le budget, le gouvernement n'a-t-il pas déclaré, à la suite des cyberattaques qui ont touché les hôpitaux de Dax et de Villefranche en février 2021, « qu'aucun projet ne pourra désormais faire l'objet d'un soutien de l'Etat si une part de à 5 à 10 % de son budget informatique n'est pas dédiée à la cybersécurité ». Même si cette évolution marque une prise de conscience notable, sa pertinence reste discutable. Partant du principe que le budget alloué au SI est d'en moyenne 1,5% du budget global d'un établissement de santé, ce qui reste sous-dimensionné, cela implique de grignoter sur un budget déjà restreint. Négocier pour une hausse du budget SI pourrait être la solution, mais ce n'est pas si simple étant donné que beaucoup de structures de santé fonctionnent déjà à budget contraint et ce depuis des années. Un cercle vicieux…

Au travers de programmes nationaux, le gouvernement met à disposition un certain nombre d'aides financières permettant d'initier les grands chantiers de sécurité. Les ARS et les GRADeS communiquent en ce moment même sur une nouvelle enveloppe de 10 millions d'euros (à l'échelle nationale) destinée au financement des établissements sanitaires pour la réalisation d'exercices cyber. Ce sont d'excellentes nouvelles, qui suivent le plan France Relance de l'ANSSI, mais la problématique de la maintenabilité dans le temps se pose toujours, surtout lorsqu'il s'agit de l'acquisition de solutions logicielles ou de la mise en œuvre de processus récurrents. Qu'en sera-t-il dans quelques années ? Les choses évoluent, certes, mais espérons la mise en place, par les pouvoirs publics, de mesures pérennes à la hauteur de l'enjeu. Une instruction ministérielle à paraître devrait imposer à chaque établissement la réalisation annuelle d'exercices de continuité d'activité. C'est clairement prioritaire, comme unique méthode pragmatique de riposte à moyen-terme. Il va falloir organiser ces exercices, les installer dans la durée et en tirer les enseignements. Encore du travail pour le RSSI !

On peut aisément conclure qu'il ne peut

y avoir de sécurité sans gouvernance, ni de gouvernance efficace sans sponsor, sans animation, sans un chef d'orchestre visible, entendu et entouré, œuvrant dans le cadre d'une stratégie partagée et d'une trajectoire financée. La pertinence de la gouvernance constitue un levier essentiel dans le renforcement de la résilience des établissements face au contexte de croissance des cyber menaces. Il convient d'y attacher une importance toute particulière, nos expériences le démontrent !

WELIOM

02 51 80 05 33
contact@weliom.fr
www.weliom.fr

4. LES PROJETS DU RSSI

Ce découpage vaut ce qu'il vaut mais il faut bien en proposer un. Il évolue constamment : dans la première édition de l'ouvrage sur la SSI des établissements de santé (2012) j'avais dénombré 9 projets majeurs alors que dans la seconde édition (2018) j'en ai mentionné 15. Le plus important est d'être certain d'adresser tous les grands sujets, même si aucune action / projet ne sont en cours sur certains des items. Il pourrait presque s'agir d'un schéma directeur, à l'estimation financière près.

La liste des projets s'articule autour de 6 grandes familles.

4.1 Le projet chapeau

4.1.1 Certification ISO 27001

Il s'agit du projet de certification ISO 27001. Le RSSI est le pilote de ce projet qui est très structurant pour une DSI. Attention à ne pas sous-estimer la charge de travail à la fois en BUILD et en RUN, tout particulièrement les effets de la montée en maturité des équipes qui doivent clairement s'approprier le sens de « système de management ». L'ouvrage qui a longtemps fait référence sur le sujet est celui d'Alexandre FERNANDEZ-TORO, même s'il n'a pas eu de mise à jour depuis les dernières évolutions de la norme à l'heure d'écriture de ces lignes.

Dernier point : ce projet est le seul pour lequel, en principe, le RSSI assume une part de la MOA et de la MOE : il est MOA du dispositif global, mais MOE du pilotage du SMSI.

4.2 Les projets techniques

Il faut mentionner le très riche corpus documentaire[1] produit et régulièrement tenu à jour par l'ANSSI.

4.2.1 Sauvegarde / restauration

Cela consiste à déployer, maintenir et superviser une architecture de sauvegarde des données. Ce projet est d'une grande complexité technique, les infrastructures mises en place ont une durée de vie qui excède rarement 3 années. Les attaques de type ransomware ont rendu ce projet crucial et ont modifié substantiellement le cahier des charges.

1 https://www.ssi.gouv.fr/administration/bonnes-pratiques/

4.2.2 Bloc d'accès

Il s'agit de l'infrastructure qui isole le LAN de l'Internet : pare-feu, proxy, boitiers VPN, etc.

La question de savoir si les flux internes seront filtrés par les mêmes équipements fait partie des sujets à instruire en priorité. Les accès fournisseurs pour la télémaintenance constituent également un point à sécuriser. Un Bloc d'accès est devenu extrêmement complexe, surtout dans un CHU support de GHT avec la maîtrise des flux inter-établissements voire l'hébergement HDS de certains de leurs SI.

4.2.3 Sécurisation du parc

Il s'agit de l'ensemble des dispositifs qui visent à faire en sorte qu'un équipement connecté au LAN (filaire ou Wifi) respecte une hygiène de base de connexion : OS à jour, AV à jour, supervision, etc.

La difficulté principale concerne les PC qui sont hors du scope de la DSI : biomédical, services techniques, médecins libéraux, chercheurs, etc.

4.2.4 Protection AV

Il s'agit de toute l'architecture à mettre en place pour assurer une protection antivirale correcte. Il y a 15 ans, cela se résumait à des AV déployés sur les PC et les serveurs mais les architectures se sont considérablement complexifiées et réclament une charge de supervision constante.

4.2.5 Protection du réseau

Il s'agit des sujets « classiques » de redondance physique des réseaux (double adduction, doublement des cœurs de réseau dans des locaux distincts, etc.) et de protection logique (802.1x). Le volet physique est à intégrer en amont dans tout projet BTP.

4.2.6 Chiffrement

Terme générique qui regroupe à la fois la gestion des certificats https, la messagerie sécurisée, le recours à des plateformes de dépôts chiffrés, etc. le chiffrement éventuel d'ordinateurs portables, le chiffrement des sauvegardes (quasi systématique en 2023) …

4.2.7 Protection du Cloud

Encore un terme générique qui traite de la protection des solutions logicielles en Saas. Ce sujet devient majeur avec les questions de souveraineté et l'abrogation du Safe Harbour.

FACE AUX CYBERMENACES ? SANCTUARISER LES DONNÉES !

Par les équipes du MIPIH

Approche métier : Point de vue du MIPIH

Les attaques informatiques dans le domaine de la santé se multiplient. Chaque mois, l'actualité nous révèle un incident mettant en situation de blackout un établissement de santé. La prolifération des cyber-attaques (virus, rançongiciels, logiciels malveillants, …) a multiplié les risques d'intrusion et de corruption des données dans ce secteur d'activité. Dans ce contexte, la mise en œuvre d'une stratégie comme l'anticipation, permettant de garantir une reprise de son système d'information dans des conditions saines, est importante. Pour cela, disposer d'un système de sauvegarde fiable afin de redémarrer en toutes circonstances, est primordial.

La **sauvegarde** est la **pierre angulaire du système d'information** des établissements de santé pour faire face aux enjeux de la perte des données.

1. La règle de sauvegarde 3-2-1

Les bonnes pratiques préconisent de mettre en œuvre une stratégie de « Sauvegarde 3-2-1 » dont le précepte est : une simple sauvegarde des données ne peut pas suffire à protéger ses informations. Pour augmenter ses chances de récupérer des données perdues ou corrompues, la « Sauvegarde 3-2-1 » est une solution. Règle fiable qui réduit au maximum la possibilité de perdre ses données sensibles.

3 - Conserver 3 copies de toutes ses données : 1 primaire et 2 sauvegardes.

La copie primaire n'est pas à considérer comme une sauvegarde. Elle représente les données principales de production. En toute logique, 2 copies des données ne sont pas satisfaisantes. En effet, il y a un risque élevé que les données de production et la copie de sauvegarde soient situées au sein du même lieu physique. Une défaillance ou une perte d'intégrité des locaux entrainerait la perte des données.
Cette première règle s'associe bien sûr à la fréquence de sauvegarde des données. Préserver une copie des données est une priorité ; mais les restaurer est tout aussi important. La sauvegarde doit s'accompagner de tests de restauration afin de garantir que les données pourront bien être récupérées en cas de sinistre.

2 - Conserver ses données sur 2 types de supports différents.

Cette règle stipule que les 2 copies ne doivent pas être sur un même support. Il est évident qu'en cas de problème de ce dernier, les 2 copies de sauvegarde seraient perdues.
De même, en lien avec le point suivant, les 2 supports ne doivent pas être localisés au même endroit.

1 - Stocker 1 copie des données, hors site.

Les solutions de sauvegarde hors site sont nombreuses : disque dur externe, un NAS portable, des bandes magnétiques… Mais la gestion de ces supports physiques peut devenir vite fastidieuse et chronophage (intendance et manipulations).
Certains établissements ont la chance d'avoir 2 locaux distincts mais souvent espacés de moins de 100 mètres. Dans le cadre d'une analyse de risque, il faut prévoir le scénario que l'établissement puisse être impacté complètement avec une répercussion directe sur les 2 locaux utilisés pour la sauvegarde.
Une solution simple et agile peut être mise en œuvre : la sauvegarde type cloud. En effet, en exportant ses sauvegardes vers un hébergeur certifié HDS (Hébergeur de Données de Santé), la règle du « hors site » est respectée.

2. La sauvegarde hors site, via un cloud sécurisé

Il existe différentes solutions pour permettre de sauvegarder ses données hors site. A l'heure des cyberattaques, cette stratégie de sauvegarde semble incontournable. L'enjeu pour les établissements de santé de disposer d'un système de sauvegarde fiable est double : *« Les données de santé permettent de prendre en charge le traitement des patients et d'améliorer leur prise en charge lors des situations d'urgence médicale. Il est donc primordial de ne pas les perdre afin d'éviter une perte de chances pour le patient. Le 2ème enjeu est de pouvoir mener un PRA, dans les cas les plus extrêmes (destruction de datacenter, crypto-virus, malveillance ou erreur humaine) »*, témoigne Guillaume BUES, Responsable de la sécurité du système d'information au centre hospitalier des vallées de l'Ariège - GHT des Pyrénées Ariégeoises.

Il faut garder en tête que l'objectif de ces sauvegardes est de **garantir le redémarrage de son activité dans un environnement sain avec des données fiables.**

Mais comment garantir la fiabilité de ces données si elles sont localisées sur le même site que celui subissant la cyberattaque ?

Dès lors, l'utilisation du cloud répond à cette exigence de sauvegarde hors site. Dans le cas de données sensibles comme les données de santé, il est important de choisir un **hébergeur certifié HDS** et **souverain.** Ainsi cela permet de bloquer la captation des données, via des réglementations extraterritoriales qui peuvent notamment autoriser une administration étrangère hors UE, disposant d'un mandat, d'accéder aux données hébergées dans les serveurs informatiques situés dans d'autres pays.

Sanctuariser ses données en passant par un hébergeur certifié HDS, offre plusieurs avantages importants :

- Une **simplicité** dans sa mise en œuvre car les couches techniques et l'exploitation sont prises en charge par l'hébergeur.
- De **très faibles coûts de stockage** dû au fait que l'hébergeur prend en charge le matériel et la mise en œuvre des technologies avec des coûts optimisés. De plus, les moyens et les ressources sont mutualisés.
- Le **coût d'investissement** est pris en charge par l'hébergeur. En effet, l'établissement va « consommer » un service de sauvegarde externalisée.
- Une **garantie de redondance** de la sauvegarde qui permet de répliquer l'information sur au moins 2 sites distants. Ainsi, si un site est défaillant, la sauvegarde est toujours accessible en temps réel sur l'autre site.
- Une **scalabilité de l'espace de stockage** de sauvegarde qui va s'adapter au rythme des demandes. Cette scalabilité horizontale garantit l'ajout de nouveaux serveurs sur l'infrastructure existante de manière transparente pour répondre à la demande.
- Une **sécurité renforcée** de ses sauvegardes par l'hébergeur grâce aux exigences du référentiel HDS, au Plan d'Assurance Sécurité de l'hébergeur, aux audits réguliers de sécurité, aux experts sécurités, …
- Une **intégrité des données sauvegardées** pour garantir leur fiabilité à travers le contrôle des erreurs et la vérification des accès habilités à ces données.

• Une **traçabilité** sur toutes les actions effectuées sur ces sauvegardes afin de savoir qui fait quoi comment et quand.
• Une **accessibilité** à la sauvegarde 24/7 avec une organisation de l'hébergeur qui propose en complément un service d'astreinte. De plus, l'hébergeur gère toutes les défaillances matérielles grâce à la redondance de son infrastructure et la présence d'experts techniques par domaine.

3. La sauvegarde des données dans le cloud, avec le protocole S3

Le cloud est une solution simple, mais comment mettre en œuvre cette sauvegarde externalisée ?

Le protocole S3, ou stockage objet, est la solution idéale qui allie **souplesse, sécurité, disponibilité et robustesse.**

En effet, le stockage objet propose, à bas coût, des espaces de stockage (bucket) où les sauvegardes peuvent utiliser le modèle objet. Ainsi, chaque objet sauvegardé va pouvoir s'appuyer sur les caractéristiques du stockage objet, à savoir :

• Une **évolutivité** de l'espace de stockage sans limite
• La **géodistribution** de la sauvegarde sur plusieurs sites distincts
• L'utilisation de la métadonnée pour définir la **propriété** de chaque objet
• Un identifiant unique pour restaurer plus **rapidement** une donnée
• Une **immuabilité** des sauvegardes par la gestion des versions de sauvegarde

Un espace de stockage compatible avec la technologie stockage objet permet de proposer un service de sauvegarde simple, non intrusif et qui **s'adapte à la politique de sauvegarde de l'établissement**. En effet, le stockage objet est une solution compatible avec tous les logiciels majeurs du marché (Veeam, Rubrik, CommVault, Cohesity, NetBackup, …). Dès lors, il est possible d'intégrer le plan de sauvegarde de l'établissement de santé en mettant en œuvre l'envoi externalisé des sauvegardes avec le protocole S3 vers l'hébergeur certifié HDS.

4. De la sauvegarde externalisée au PRA externalisé, il n'y a qu'un pas !

La sauvegarde est un point crucial dans la stratégie et l'analyse de risque pour un établissement souhaitant assurer la sécurité de ses données. Mais la restauration en est

un tout aussi important. Si nous allons plus loin dans le raisonnement, un établissement, qui a opté pour une externalisation de ses sauvegardes, ne devrait-il pas aussi externaliser sa restauration dans le cadre d'un PRI (Plan de Reprise Informatique) * ?

**Un PRI est l'ensemble des mesures prévues pour rétablir l'activité du SI après interruption suite à un incident.*

Dans le cas où un établissement a subi un incident majeur de type cyberattaque, et malgré ses sauvegardes hors site, il ne serait pas autorisé à restaurer ses sauvegardes sur site. En effet, il serait inconcevable de restaurer les données sur une infrastructure défaillante. Il en est de même si l'établissement a subi un évènement ou une catastrophe naturelle (incendie, inondation, ouragan, séisme, …). Dès lors, la sauvegarde dans le cloud chez un hébergeur certifié HDS pourrait permettre de restaurer le SI dans un environnement sain et dans un datacenter extérieur à l'établissement.

La reprise du SI après un sinistre permettrait à l'établissement d'avoir accès **rapidement à la restauration** de ses machines sur une infrastructure extérieure. *« Devant le volume de données sauvegardées, en cas de PRA, la rapidité de restauration devient un élément important »* souligne Guillaume Bues. Cela n'implique aucune contrainte matérielle pour l'établissement qui va s'appuyer sur une nouvelle **infrastructure virtualisée chez l'hébergeur.**

Le PRA est donc très dépendant des choix stratégiques de l'établissement en termes de préservation des données de santé et de continuité d'activité. Il est, en définitive, l'étape suivante d'une démarche de sauvegarde externalisée.

mipih

05 34 61 50 00
contact@mipih.fr
www.mipih.fr

4.3 Les projets fonctionnels

4.3.1 Traçabilité

Tout actif technique ou fonctionnel composant du SI produit des traces : accès au DPI, connexion sur un PC, navigation Internet, traces serveurs, actifs complexes, logiciels techniques DSI, etc. Ces traces impactent à la fois le volet réglementaire (présence de l'information de traçabilité dans une charte), technique (durée maximale de conservation) et fonctionnel (qui a accès aux traces et pour faire quoi).

4.3.2 SIEM

Indissociable de la question des traces, la mise en place d'un SIEM fait partie des briques indispensables. Sa couverture et son lien avec les équipes de remédiation constituent pour autant des sujets complexes : c'est bien beau de repérer des tonnes d'anomalies, mais si c'est pour les laisser en plan faute de bras pour corriger…

4.3.3 SOC

Indissociable d'un SIEM, le centre de pilotage des alertes est encore un sujet pour lequel couverture et niveaux de services sont des sujets complexes. SIEM et SOC constituent des sujets à part entière et pourraient faire l'objet d'un guide dédié.

4.3.4 Habilitations

Sujet extrêmement complexe et qui a fait l'objet d'un Guide cyber dédié. Voir annexes «13.2 Ouvrages techniques».

4.3.5 Démarches internes de type Plan Blanc

Dans le cadre d'une démarche interne Plan Blanc, il est de plus en plus courant de voir que le risque cyber fait partie des scénarii envisagés. Les pouvoirs publics sont en train d'intégrer des exercices de crises dans les prérequis à certains financements, la différence entre exercice de crise, plan blanc, PCA-PRA étant un sujet à part entière qui nécessite plusieurs pages pour en décortiquer l'articulation.

4.4 Les projets mixtes

4.4.1 PCA-PRA

Il s'agit de l'ensemble du dispositif, à la fois organisationnel et technique, qui vise à minimiser la probabilité d'une panne, en réduire la durée quand elle arrivera, et réduire le retour à la normale ainsi que la charge de ressaisie des MOA.

Point important : cela ne se résume pas à doubler des serveurs, il y a aussi et surtout les procédures dégradées métier. Autre point important : on oublie généralement la téléphonie et le site de repli de la DSI en cas de crash majeur. Ce sujet fait l'objet d'ouvrages entiers.

4.4.2 IAM

Souvent pris comme un projet technique (il est vrai que les briques SSO et méta-annuaire sont très techniques), il s'agit en réalité d'un projet global qui vise à nettoyer la gestion des identités des personnels ayant un lien contractuel avec l'établissement (pas seulement les agents), afin d'assurer à la fois une création des ID dans le SI en quasi temps réel, une attribution des habilitations de façon quasi automatisée, et une révocation des ID et habilitations à J+1 du départ des personnes de la structure.

Il s'agit d'un des projets SI les plus complexes qui soit.

4.4.3 Archives

Curieusement, ce projet n'est pas identifié comme requérant l'intervention du RSSI : c'est pourtant un sujet typique ayant un fort volet SSI. Attention, sous des aspects simplistes, ce projet est en fait d'une très grande complexité : stockage des données à objectif du siècle, épuration avant archivage, décommissionnement, valeur probante ou pas (et avec quelles technologies sur le long terme), etc.

4.5 Les projets de conformité

4.5.1 HDS

La certification HDS implique une certification ISO 27001, elle en est une surcouche essentiellement documentaire. Son intérêt légal et fonctionnel est en débat.

Le certification HDS est en train d'évoluer

avec une v2, qui règle certains « défauts de jeunesse » de la v1 et notamment l'activité 5.

4.5.2 CAC

La certification des comptes a un impact sur le SI et notamment sur les procédures de création / modification / suppression des comptes à privilèges, à la fois fonctionnels et système. Elle a également un impact important sur la définition et la révision des politiques d'habilitation aux données métier.

En ce sens, une certification ISO 27001 est un plus vis-à-vis des CAC externes, car elle conduit à mettre en œuvre un processus de contrôle interne sur le SI.

4.5.3 Directive NIS

Pour les établissements désignés OSE (Opérateur de Service Essentiel), il s'agirtde 23 règles à mettre en œuvre sur les SIE (Systèmes d'Information Essentiels) recensés en interne. Il n'y a quasiment aucune contrainte sur le nombre et la nature des SIE à déclarer, et il y a un bénéfice clair à utiliser la certification ISO 27001 pour cocher pas mal de case de la directive NIS.

4.5.4 Certifications ISO sectorielles

D'autres services ou pôles ont eux-mêmes des impératifs de certification (ISO 15189 pour les laboratoires de biologie) dont une partie concerne l'informatique : une certification ISO 27001 interne permet également de cocher pas mal de cases au sein de ces certifications sectorielles.

4.5.5 Exigences ministérielles

Régulièrement, le Ministère émet des recommandations ou des exigences qui se traduisent par des indicateurs à remonter, des audits ou contrôles à réaliser. Encore une fois, une certification ISO 27001 de la DSI permet de gagner du temps.

4.6 Les projets en attente de classification

4.6.1 La protection ransomware

Sujet du moment, la protection contre les ransomwares a ceci de particulier qu'elle emprunte à pas mal des projets susnommés : protection antivirale, protection périmétrique, gestion des accès fournisseurs, procédures dégradées, Plan

Blanc, etc.

Les évolutions des modes d'attaque sont frappantes : pour exemple, alors que les ransomwares de la génération 2021 chiffraient chaque fichier et pouvaient être détectés par des modules résidents dans les baies de disques, les dernières générations ne chiffrent que les octets d'en-tête de chaque fichier, rendant leur détection beaucoup plus aléatoire car fonctionnant en mode signal faible.

4.6.2 La cyber assurance

Ce sujet pourra, à terme, rejoindre la conformité ou constituer un domaine à part. A l'heure d'écriture de ces lignes, il existe assez peu d'informations sur ce sujet. Les assureurs qui avaient initialement investis en masse le marché avec des offres adaptées se sont pour certains retirés tandis que d'autres revoyaient le périmètre des garanties.

4.6.3 Le juridique

Le RSSI est en veille juridique permanente et doit notamment produire des annexes à intégrer aux contrats et listant les préconisations SSI.

La question de la relecture des contrats
Le RSSI doit prendre garde à cette charge de travail extrêmement chronophage : mieux vaut maintenir un corpus documentaire d'annexes (qui évoluent selon les remarques remontées par les interlocuteurs internes et externes) que de relire systématiquement tous les contrats : une équipe entière de RSSI n'y suffirait pas.

CYBERSÉCURITÉ & SANTÉ : « GOUVERNANCE ET PAM, LE DUO GAGNANT »

Par François LANCEREAU, expert santé chez Wallix

Approche métier : Point de vue de WALLIX

Pour sécuriser les infrastructures informatiques des établissements de santé, il est nécessaire de disposer de budget adapté et de compétences dédiées. Sans moyens humains, les projets ne pourront pas être menés efficacement. L'accent doit donc être mis sur le recrutement mais aussi sur la sensibilisation et la formation de tous les métiers de l'hôpital. La cybersécurité doit désormais être une affaire de gouvernance.

1. Que faire pour réduire le risque cyber dans les établissements de santé ?

Les budgets actuels des hôpitaux ne sont pas suffisants, bien que la situation s'améliore, notamment depuis la pandémie pendant laquelle il y a eu une véritable prise de conscience de la vulnérabilité des hôpitaux et des conséquences dramatiques que peuvent avoir les cyberattaques. On se rappelle notamment du décès d'un patient suite à la cyberattaque de l'hôpital de Düsseldorf en Allemagne. Les pouvoirs publics du monde entier débloquent désormais des aides financières pour aider les hôpitaux à se sécuriser.

Pour comprendre la vulnérabilité de certaines structures de santé, il faut garder en tête que pendant longtemps, les « DSI » étaient en fait que des médecins avec plus ou moins d'appétence pour l'informatique. Cette organisation a beaucoup évolué depuis ! Soit certains de ces médecins sont devenus des experts en informatique, soit on a attribué ce poste à une personne dont c'est le métier : le DSI (Directeur des Systèmes d'Information). En plus du DSI, les établissements de santé ont petit à petit recruté un spécialiste de la cybersécurité : le RSSI (Responsable de la Sécurité des Systèmes d'Information). Le processus avait commencé avant la pandémie de Covid, puis, en raison des différentes attaques ayant eu lieu dans le secteur pendant et depuis la crise, le RSSI est devenu une véritable nécessité.

Cependant, avant la crise Covid, le rôle du RSSI était limité. La direction, n'ayant pas mesuré les conséquences potentiellement dramatiques d'une cyberattaque, ne permettait pas au RSSI d'avoir le budget nécessaire pour appliquer ses recommandations. C'est seulement une fois la catastrophe survenue que la direction prend conscience de l'importance de la cybersécurité. Imaginons qu'un hacker arrive à stopper le système de ventilation

des blocs opératoires, ils doivent être immédiatement fermés car un bloc non aéré est un bloc non stérile et si un patient est sur la table à ce moment-là, c'est sa vie qui est en jeu. Beaucoup de cyberattaques auraient pu être évitées ou du moins endiguées si la cybersécurité était un sujet de gouvernance.

La crise Covid a joué un véritable rôle de prise de conscience et d'accélération de la transformation numérique des établissements de santé. Le RSSI est désormais écouté mais pour que la cybersécurité soit maximale, il faut encore que ce sujet soit saisi de manière globale. Le RSSI a un rôle de préconisations mais il est impératif qu'il ait l'adhésion du DSI, des dirigeants, et de tout le personnel. Chaque personne travaillant dans l'établissement de santé doit pouvoir être sensibilisée aux bonnes pratiques de cybersécurité et formée aux solutions que va mettre en place le RSSI.

La dernière étape pour réduire au maximum le risque de cyberattaques est la mise en place d'une solution de sécurisation des accès et des identités numériques dite de PAM (Privileged Access Management). C'est désormais un must have pour tous les établissements de santé - comme les organisations du monde entier, tout secteur confondu. C'est le seul moyen de savoir qui se connecte à l'infrastructure informatique (humains, machines ou applications), de s'assurer de l'identité de cette personne / machine / application, et de traquer tout ce qu'elle fait. Ainsi, en cas de suspicion d'intrusion par un hacker, la cyberattaque est potentiellement immédiatement stoppée.

2. Et la réglementation dans tout ça ?

La réglementation (RGPD, NIS 2…) est en effet importante car elle permet d'avoir des standards de cybersécurité et oblige les directions d'établissements de santé les plus récalcitrantes à ériger la cybersécurité à l'ordre des priorités. C'est une base mais encore une fois, appliquer la loi ne sera pas suffisant si les budgets ne suivent pas et si la cybersécurité ne devient pas une affaire de gouvernance. Pour réduire le risque cyber à son maximum, il faut que tout l'hôpital s'y mette et que les pouvoirs publics débloquent des fonds pour la modernisation des infrastructures numériques des établissements de santé.

L'arrivée du European Cyber Resilience Act est un complément aux normes déjà en place. L'une des failles de sécurité majeures dans les hôpitaux est constituée par le matériel biomédical qui aujourd'hui comprend toute sorte d'objets connectés. Le European Cyber Resilience Act va permettre que tous les objets connectés vendus en Europe soient sécurisés « by design », c'est-à-dire dès leur conception. Cela va rajouter une couche supplémentaire de cybersécurité et faciliter le travail du RSSI qui jusque-là devait faire en sorte que chaque accès à un objet connecté soit sécurisé, l'objet lui-même représentant une faille potentielle. Ce sont désormais les fabricants qui s'adaptent aux besoins en cybersécurité des établissements de santé et non l'inverse. D'ailleurs, chez WALLIX, nos technologies de sécurisation des accès et des identités numériques étant intégrables « by

design » dans les produits des constructeurs, nous sommes d'ores et déjà en contact avec eux. La chaîne évolue !

Cependant, cette loi ne soustraira pas les hôpitaux à l'implémentation d'une solution de sécurisation des accès et des identités numériques de type PAM. Cela restera toujours un must have qui permet de se mettre en conformité avec de nombreux éléments des réglementations de cybersécurité en vigueur. D'une part, il faut avoir à l'esprit que dans les hôpitaux, il existe de nombreux appareils connectés obsolètes du point de vue de leur couche numérique, comme, par exemple des scanners, des mammographes, des moniteurs. Ils représentent des points de vulnérabilité qu'il faut donc gérer et sécuriser. D'autre part, les accès numériques à sécuriser ne sont pas uniquement ceux des objets connectés, mais aussi les flux induits par le télétravail, l'utilisation de services cloud, la maintenance du biomédical, la GTB, la visioconférence… La sécurisation de tous les accès au système d'information de l'établissement de santé, qu'ils soient « machines » ou « humains » est un enjeu vital.

WALLIX
CYBERSECURITY SIMPLIFIED
06 07 66 43 93
flancereau@wallix.com
www.wallix.com

5. LE QUOTIDIEN DU RSSI

S'il est un métier bizarre, c'est bien celui de RSSI : ne fait rien lui-même mais incite les autres à faire, contrôle et débusque des dysfonctionnements, passe une grande partie de son temps à parcourir la presse et les sites spécialisés, tout en n'étant responsable de rien. Dit comme cela c'est un peu étrange, mais la fonction de RSSI est essentielle, autant que peuvent l'être les fonctions de contrôles internes. Factuellement, ce sont ces fonctions hyper transverses qui ont le plus fait progresser la maturité organisationnelle ces 20 dernières années.

ISO 9001 dans les services de l'Etat

Que l'on songe deux minutes à l'état de certains services de l'État il y a à peine 30 ans (horaires décorrélés avec les besoins des usagers, procédures kafkaïennes, etc.) : les normes ISO 9001 sont passées par là et dans la plupart des cas, l'usager est maintenant au centre des processus. Qui souhaiterait en 2022 revenir à la façon dont on devait acheter un billet de train dans les années 80 ?

5.1 La répartition du temps

Idéalement, un RSSI passe 30 % de son temps à faire de la veille sous toutes ses formes, 30 % de son temps à gérer ses propres projets (ISO 27001, dossiers en propres, instructions de dossiers sur demande, etc.), le reste étant passé à gérer les urgences, les interventions en réunions diverses, les animations d'instances, etc.

Le plus difficile est, clairement, d'arbitrer entre les urgences et le travail de fond. La masse de travail qui pèse sur un RSSI, même dans un établissement de taille moyenne, fait qu'il n'a pas d'autres choix que de déléguer certaines de ses actions récurrentes : contrôles, audits, points de mesure, formations, sensibilisation, etc. De faiseur, il passe rapidement à la mise en place de processus dont il contrôle d'abord lui-même le fonctionnement (contrôle dit de niveau 1) avant de demander aux délégataires de procéder eux-mêmes au contrôle de la fonction déléguée et se positionner ainsi en contrôle de niveau 2.

Un autre critère de maturité de la fonction RSSI

En sus de sa position hiérarchique, il est possible d'examiner la cartographie de ses contrôles : il peut n'en avoir que très peu et les faire lui-même, il peut en avoir beaucoup, il peut en avoir délégué tout ou partie, il peut se positionner essentiellement en contrôle de niveau 2.

Dans ce contexte de délégation toujours croissante, la veille devient un enjeu de survie s'il ne veut pas devenir rapidement incompétent... d'où la répartition des taches évoquées ci-dessus. La boucle est bouclée.

5.2 Le choix d'une méthode d'AR

Curieusement ce sujet fait souvent débat : MEHARI, EBIOS, EBIOS RM ?

Quelles recommandations ?
Je n'entends plus jamais parler de MEHARI. J'entends quand même que pour les OIV et OSE, le recours à EBIOS RM « méthode ANSSI » est recommandé. Avant la sortie de la version RM, c'est EBIOS qui était « plus que recommandé » jusqu'à ce que les pouvoirs publics réalisent la lourdeur du bazar.

En fait, cela n'a aucune importance : pour être clair, seul le respect de l'ISO 27005 est véritablement une contrainte, et cette dernière n'impose rien de plus que de lister des actifs, des menaces, de les évaluer (noter), de les traiter (réduction, transfert, etc.), point final.

La meilleure méthode est celle :

- avec laquelle le RSSI est à l'aise ;
- qui est reproductible (la dérouler 10 fois donnera 10 fois le même résultat à un pouième près) ;
- qui est révisable en interne sans que cela coûte 10 jours de consultant hyper spécialisé (donc hyper cher) à chaque révision, qui est à minima annuelle.

Si vous avez été formé à EBIOS et que la méthode vous est familière, aucun souci. Si vous ne la connaissez pas et que vous estimez avoir d'autres priorités que de batailler avec des documents Excel complexes à chaque mise à jour, un bête tableau avec 10 colonnes vous suffira.

Certification ISO 27001 et méthode AR
Il m'est arrivé de tomber sur des consultants me soutenant mordicus que sans AR déroulée à la sauce EBIOS pur jus, adieu la certification. C'est un mensonge. Et ce n'est pas près de changer selon moi, puisque le sens de l'histoire est de se raccrocher à des normes (ISO 27005 dans le cas présent) car ce sont les seules à faire consensus (c'est même une des significations d'une norme).

5.3 Les actions et leviers

5.3.1 Les 3 temps

Les 3 grands temps du RSSI sont : avant le sinistre, pendant le sinistre, et après le sinistre.

Avant le sinistre, le RSSI a peu de pouvoir en dehors de la négociation : on est sur du soft power, de la force de conviction, de la négociation raisonnée. Les seules mesures de sécurité qu'il est possible de mettre en place sont celles qui sont acceptées par toutes les parties : MOA, DSI et RSSI. Au-delà, le RSSI dispose de peu de marge de manœuvre. Sa seule bouée de secours est : la MOA est seule propriétaire de ses risques - et il est fortement conseillé de tracer les échanges.

Pendant le sinistre (attaque, panne, fuite de données, etc.), le RSSI a un rôle de :

• communication avec la MOA et l'extérieur de l'établissement : ANSSI, Ministère, équipes de cyber veille, etc.
• coordination avec les autres équipes de crise internes à l'établissement : plan blanc, etc. ;

Le moment du sinistre est un des rares où le RSSI peut sortir de son strict rôle de conseil et imposer des éléments de sécurité « temporaires » (et dont l'objectif non avoué est qu'ils deviennent définitifs). Le mode soft power n'est pas vraiment utile pendant cette phase.

Enfin, après le sinistre, le RSSI revient en mode négociation : la seule différence avec la première phase est qu'il est beaucoup plus écouté et par beaucoup plus de monde (le chiffre étant proportionnel au niveau de perturbation rencontré pendant le sinistre), mais cela ne dure pas longtemps : la fenêtre de tir s'étale rarement au-delà de 3 à 6 mois. Et jusqu'au prochain cycle.

Déjeuner à la cantine
Une boutade pour la route...
Avant le sinistre, le RSSI déjeune seul.
Pendant le sinistre, il déjeune avec le top management.
Après le sinistre, il déjeune seul et dos au mur du fait de tout ce qu'il a imposé à tout le monde.

5.3.2 Focaliser sur les 3 situations

Globalement, le RSSI peut classer les situations en 3 grandes catégories.

Il y a d'abord le « connu connu » : ce que l'Organisation sait qu'elle sait.

Il s'agit par exemple des cœurs de réseau dont la DSI sait qu'ils sont redondés, des procédures d'utilisation des automates de laboratoires que les biologistes connaissent, des alimentations électriques que les services techniques savent redondées, etc. Ces éléments ne présentent pas de risque majeur, ils sont régulièrement audités ou contrôlés, etc.

Il y a ensuite le « connu inconnu » : ce que l'Organisation sait qu'elle ne sait pas. La DSI ne sait pas combien de PC sont non-protégés par un AV (mais elle sait qu'il y en a), le service de Réanimation sait que certains des équipements sont hors contrats de maintenance mais ne connaît pas le MTBF (Mean Time Between Failure ou temps moyen avant panne). Les experts téléphonie savent qu'ils ont très peu de visibilité sur la redondance téléphonie de l'opérateur, etc. Ces situations sont sources de risques et doivent focaliser l'attention du RSSI : audit, réunion, plan de remédiation, risque résiduel accepté, etc. En d'autres termes, il faut que quelqu'un s'occupe du machin, qu'il ne soit pas laissé sans surveillance.

Enfin, il y a l'« inconnu inconnu » : ce que l'Organisation ne sait pas, et qu'elle ne sait pas ne pas savoir. Cela peut être un service métier qui a basé tout son fonctionnement sur des fichiers Excel non sauvegardés sur un PC au fond du couloir, un autre qui utilise comme système de communication critique en temps réel le mail, un troisième qui base tout son système de rappel en garde sur des sms, etc. L'Organisation n'a aucune connaissance de la situation, et encore moins du niveau de risque que cela engendre. Ce

sont les pires situations, les plus difficiles à débusquer, et qui justifient à elles seules que le RSSI s'immisce partout, discute avec tout le monde.

Le coût d'un café

Vous n'imaginez pas tout ce qu'un RSSI peut apprendre, juste en traînant dans la salle de pause pendant le café, voire en offrant des cafés à un médecin, un chef de service, un cadre, un ingénieur, etc. Les Organisations ne sauront jamais ce que le prix d'un seul café leur aura évité…

Parmi l'« inconnu inconnu », il y a un grand classique : la distorsion entre le SLA de la DSI (son temps moyen de remise en service après panne, ou ses plages horaires de maintenance programmée des éléments d'infrastructure) et ce que les MOA en savent ou en perçoivent : combien de fois suis-je tombé sur une MOA qui, après une panne de quelques heures de la messagerie, m'avoua qu'elle ne pensait pas que la messagerie pouvait tomber en panne (authentique).

5.4 Le lien avec le DPO

Autant le positionnement du DPO ne fait pas débat (il ne peut pas être dans la DSI car elle met en œuvre des traitements), autant on trouve encore des débats concernant le positionnement du RSSI.

Or, leurs travaux se ressemblent comme deux gouttes d'eau : appréciation des risques, rôle strict de conseil et d'alerte, la MOA (ou le Responsable de Traitement) seul propriétaire de ses risques, etc. Pour ceux qui cumulent les 2 fonctions, il est, certains jours, quasi impossible de dire à quel moment de la journée on est RSSI et à quel autre moment DPO.

La synergie des deux postes est extraordinaire car il est rare que ce qui doit être déconseillé par l'un soit conseillé par l'autre : 2 visions différentes des mêmes sujets ou projets amènent souvent des conclusions identiques, d'où l'intérêt soit de cumuler les 2 fonctions, soit de les positionner en binôme.

Cerveau droit et cerveau gauche

Pour ceux qui ont la chance de cumuler les deux fonctions, je leur conseille d'utiliser pour émettre un avis négatif sur telle ou telle situation la moitié de leur cerveau adaptée aux circonstances, la droite ou la gauche selon les jours. Si le cerveau droit RSSI ne peut pas s'opposer, le cerveau gauche DPO lui vient en aide.

5.5 Les dérapages

Parmi les dérapages ou incompréhensions que l'on peut rencontrer lors d'une prise de poste, on trouve en général les travers suivants.

5.5.1 La technique pour la technique

Il s'agit du RSSI qui pense que la technique résout tout et qu'il faut répondre aux besoins de sécurité par une débauche de matériels, logiciels en tout genre. Dans les secteurs où le RSSI dispose d'un budget confortable, c'est assez courant. Or, le meilleur logiciel du monde s'installe, se supervise et alerte de non-conformités qu'il faut bien traiter : sans ressources RH, il ne sert à rien si ce n'est constater que votre SI est aussi troué qu'un gruyère. Le RSSI qui tombe dans ce travers ne sort jamais de la soute.

La solution est bien entendu de faire la part entre la technique (qui, au passage, existe souvent en version open source totalement gratuite et d'excellent niveau) et les ressources humaines, internalisées ou externalisées.

5.5.2 L'art pour l'art

Travers plus courant chez les jeunes RSSI, il s'agit de faire de la sécurité pour elle-même sans la replacer dans un contexte global à la fois tactique (les besoins des utilisateurs, l'état du SI, etc.) et stratégique (les budgets sur le long terme, les contraintes de l'entreprise, etc.).

Le RSSI qui tombe dans ce travers finit immanquablement par pérorer tout seul dans son bureau.

5.5.3 Sortir de son rôle de conseil

En dehors des périodes temporelles spéciales que sont l'incident et la bêtise manifeste qui peut mener à des grosses catastrophes, le RSSI doit veiller à rester dans ce rôle de conseil et d'alerte, sous peine de déborder sur la MOA alors qu'il n'est que MOE. Le mélange des genres MOA / MOE finit toujours par se retourner contre lui.

6. LES OUTILS

6.1 Les outils techniques

S'il est un domaine qui cède rapidement à la facilité de la fascination pour la technologie, c'est bien la cyber : des logiciels prétendument miracles qui vont détecter les failles avant même qu'elles impactent votre SI, basés sur de l'IA (c'est à la mode, il y a 30 ans on parlait de « systèmes experts »), des algorithmes apprenants, des IA Machine To Machine, et j'en passe.

La débauche de technologie est, en général et encore plus dans la cyber, un miroir aux alouettes pour au moins 3 raisons :

- si une technologie était vraiment la protection ultime, la théorie de l'évolution nous dit qu'il y a belle lurette qu'elle aurait raflé tout le marché et tous les clients, ce qui n'arrive pour ainsi dire jamais ; même les modules EDR accolés aux AV classiques et dont on nous rabat les oreilles depuis des années sont loin d'être la panacée ;
- un logiciel ou un matériel ne fonctionnant pas par l'opération du Saint Esprit : il faut de la ressource (RH) pour l'installer, de la ressource (encore RH) pour l'exploiter sans même parler de la ressource (toujours RH) pour effectuer de la remédiation suites aux failles relevées par ledit logiciel ; or, la plupart du temps, c'est bien la ressource RH qui fait défaut et on se retrouve à avoir dépensé des sommes folles pour installer un bazar qui finit au fond d'un tiroir ;
- dans les faits, quand les fournisseurs qui toquent à la porte avec le machin prétendument magique veulent bien réaliser un POC, souvent le POC en question est loin de tenir toutes les promesses des plaquettes marketing bien léchées ;

Je commence à détester les camemberts

Que l'on m'explique pourquoi les ingénieurs commerciaux qui cherchent à vendre leurs produits me présentent systématiquement des copies écran avec des statistiques en forme de camemberts de toutes les couleurs, histoire de me montrer que leur machin est fortiche dans la conversion tableau <=> graphique. A moins qu'ils me prennent pour un décideur qui ne connaît rien à la cyber ? Pourtant juré je ne porte jamais de costard trois pièces. Non, personnellement je préfère la bonne vieille ligne de commande, on n'a rien fait de mieux depuis les tablettes de cire.

La réalité est beaucoup moins sexy : quasiment tous les outils pour faire de la cyber au moins jusqu'à un niveau avancé existent en format open source, moyennant un peu d'huile de coude pour rentrer dedans. Le boulot d'un RSSI fonctionnel est d'avoir une vision sur une cartographie d'outils et leurs champs d'action (cela s'appelle la veille fonctionnelle), le boulot d'un expert SSI (eCS) est de savoir les mettre en œuvre pour ce à quoi ils sont destinés. Vous allez me dire que c'est un sacré boulot justement que d'intégrer des briques open source hétérogènes, et vous aurez raison. Mais vous pensez que c'est une partie de plaisir que de déployer un IDS ? Un scanner d'IoT dans un environnement LAN / VLAN segmentés à tout va ? Une console d'analyse SIEM / SOC qui corrèle les traces de l'AD avec celles du pare-feu et de 5 autres sources de données ?

Quand vous serez arrivés au bout des possibilités d'un PingCastle, d'un Suricata, d'un bête grep, quand votre capacité à remédier sera supérieure au rythme auquel

ces outils vous remontent des failles, alors à ce moment-là et seulement à ce moment-là vous pourrez aller réclamer des budgets pour acheter un truc payant. Soyons clairs, il y a des domaines de l'industrie ou du tertiaire qui sont justement au niveau où les outils payants sont nécessaires. Et il y a des équipes dans les hôpitaux qui, sur certains sujets, ont passé ce cap. Mais le schéma reste le même : d'abord on doit mettre en priorité budgétaire la mobilisation d'ETP, et ensuite, seulement ensuite, des budgets pour acheter la quincaillerie.

6.2 Les autres outils

Le RSSI et son expert SSI ont besoin de disposer d'outils, de ressources documentaires et de site Web afin de maintenir une veille technique et « conjoncturelle ».
Le lecteur trouvera en annexes une liste, forcément personnelle, forcément périssable et forcément incomplète, de ces items.

7. RÉSEAUTER

Sans son réseau, un RSSI n'est rien.

Concernant les problèmes qu'il rencontre au quotidien, quelqu'un d'autre les a rencontrés avant lui et réglés : faire appel au réseau constitue un gain de temps considérable, permet d'accélérer la veille, de ne rater aucune nouveauté, aucun texte, aucune documentation, livre blanc, etc.

Le réseau se décompose globalement en :

• réseau local : les RSSI dans la même ville, département, région ; souvent il s'agit d'un réseau non sectoriel, il y a des groupes de travail souvent pilotées par les CCI locales à peu près partout, même si elles sont souvent noyautées par les fournisseurs ;
• le réseau national sectoriel : dans la santé il existe un groupe informel de RSSI de CHU et de gros CH ;
• les clubs : on peut citer évidemment le CESIN[2];
• les associations à but non lucratif : bien entendu l'APSSIS, mais il peut y en avoir d'autres dans d'autres secteurs de l'économie ;

Faire appel au réseau est naturel, renvoyer l'ascenseur tout autant : on ne perd jamais de temps à passer 30 minutes ou plus avec un confrère au téléphone pour le dépanner.

2 https://www.cesin.fr/

8. Le volet juridique

Il est fortement conseiller au RSSI (et au DPO également) de tenir à jour une liste des textes et autres règlements qui s'imposent à sa fonction. Attention cela bouge pas mal, avec des décrets et arrêtés dans tous les sens et sur tous les sujets. A noter que cette tenue à jour est une obligation de la norme ISO 27001 (clause A.18.1.1 dans la version 2017).

Le lecteur trouvera ci-joint, en mode carte mentale, un exemple de ce recensement.

CYBERSÉCURITÉ, LA VISION JURIDIQUE

Marguerite BRAC DE LA PERRIÈRE, Avocate Associée, spécialisée en santé numérique, IT & Data, au sein du Cabinet LERINS

Approche métier : Point de vue de l'avocate

L'accélération de la numérisation au sein des établissements de santé, la multiplication des solutions logicielles et des dispositifs médicaux intégrant des applicatifs ou objets connectés, l'intensification de la coordination des soins, à l'hôpital, et avec la ville, et la multiplication des bases de données, constituent de formidables opportunités.

Des opportunités concourant à l'amélioration des conditions de prise en charge des usagers. Des opportunités constituant le terreau d'une médecine de précision, d'une prise en charge plus personnalisée.
Des opportunités d'efficience, et de rationalisation des soins, participant de la transformation de notre système de santé, et ce faisant, à la pérennisation des mécanismes de solidarité.
Des opportunités de recherches et d'innovations.

Avec cependant comme corollaires, une surexposition au risque cyber, des incidents aux impacts organisationnels, humains et financiers lourds, et des violations des données de santé, associées parfois à une diffusion sur le web ou le darkweb.

En matière de prévention du risque cyber, les défis sont bien sûr technologiques et humains :

• technologiques avec une vigilance particulière sur l'interopérabilité entre applications, et sur les solutions de sécurisation de messagerie et des accès à distance ;
• humains avec un enjeu majeur de sensibilisation ; la protection du système d'information et de ses données relevant d'un effort quotidien, à la fois individuel de chaque utilisateur, et collectif, impliquant la sécurité, et également les achats, la qualité, la conformité, la direction juridique, le DPO…

S'agissant des instruments juridiques, ils s'articulent principalement autour, d'une part, de la mise en œuvre de la protection des données et l'encadrement des prestataires, et d'autre part, de la réaction en cas de violation.

La protection des données repose largement sur le choix des prestataires et sous-traitants afin de s'assurer qu'ils présentent les garanties suffisantes[1] quant à la mise en œuvre de mesures techniques et organisationnelles appropriées[2], et sur les exigences auxquelles ils sont contractuellement soumis.

A cet égard, il appartient à l'établissement, outre les clauses obligatoires au titre du RGPD, et au titre de la réglementation Hébergeur de Données de Santé, de requérir la conformité aux référentiels de sécurité et d'interopérabilité -lesquels bien que légalement opposables[3] restent imparfaitement mis en œuvre-, mais aussi la conformité des solutions, connecteurs et services, y incluant support et maintenance, à l'état de l'art.

L'état de l'art constitue désormais d'une

1 Au sens de l'art. 28.1 RGPD
2 Au sens de l'art. 32 RGPD
3 L1470-5 CSP

notion centrale dans chaque contrat IT, dans le contexte d'un environnement réglementaire foisonnant, et d'exigences très évolutives.

La plupart des exigences relèvent de textes réglementaires, dont :

- la réglementation Hébergement de données de santé (HDS) dont le référentiel de certification est en cours d'évolution, et les enjeux de souveraineté associés ;
- la Directive NIS, transposée en droit national, ayant renforcé la cybersécurité des Opérateurs de Services Essentiels (OSE) ;
- La Directive NIS 2 récemment adoptée -à transposer en droit national sous 21 mois- concernant également les sous-traitants et prestataires de services ayant accès à une infrastructure critique.

D'autres exigences relèvent de référentiels portant des recommandations, dont récemment le Guide sur la cybersécurité des DM et DMDIV de l'ANSM.

Au regard de ce qui précède, la rédaction et négociation des contrats IT apparaissent cruciales afin de permettre à l'établissement de bénéficier d'engagements limitant les risques en matière de sécurité, mais aussi les risques de sanctions des autorités (outre celles prévues au RGPD, bientôt celles de NIS 2 similaires), et lui garantissant une évolution des solutions et services dans des conditions équilibrées, pendant toute la durée d'amortissement.

La réaction à une éventuelle cyberattaque devient, dans le même sens, un enjeu majeur, non seulement à l'égard du soutien qu'elle déclenchera, mais également au regard d'un objectif de limitation de responsabilité, étant rappelé que les incidents doivent désormais être déclarés à l'ANS[4] laquelle fera le lien avec l'ANSSI, outre, en cas de violations engendrant un risque pour les droits et libertés des personnes, notifiés à la Cnil, sans préjudice d'une plainte pénale.

Ou comment la cybersécurité est devenue un sujet presque aussi juridique que technique…

www.lerins.com

4 Décret 2022-715 du 27-04-2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information

9. Les âneries courantes

Il y a certaines erreurs de base à éviter à tout prix lorsque l'on se retrouve sur un poste de RSSI.

J'en ai moi-même commis certaines, et elles se voient surtout chez les nouveaux-venus dans la profession, à fortiori lorsqu'ils viennent d'un domaine technique (exemple : l'ingénieur réseau promu RSSI) ou d'un autre secteur (exemple : le consultant qui se retrouve RSSI en CHU). Elles sont à identifier rapidement, car elles sont coûteuses en temps, en réputation et impactent donc indirectement l'efficacité future du RSSI, quand elles ne mènent pas directement à son départ contraint ou négocié.

9.1 Parler de chiffrement homomorphe à un Directeur Général

J'avais assisté, médusé, à une intervention d'un consultant externe devant un parterre de décideurs de type DG, qui leur a décrit par le menu les rudiments du chiffrement asymétrique. Si vous voulez passer pour un obscur geek ou un doux-dingue, c'est la bonne méthode. Un RSSI doit adapter son discours à son auditoire, c'est même une de ses qualités premières.

9.2 Faire passer ses idées en force

Le job du RSSI, c'est 99 % de négociation. Les cas sont nombreux d'un RSSI qui se retrouve devant une direction (MOA, DSI, etc.) qui se contrefiche de ses recommandations, de ses préconisations. Allez au clash verbal est certainement la pire des méthodes : toujours revenir aux basiques, à savoir que le propriétaire d'un actif est propriétaire de ses risques. Le DSI se contrefiche que 80 % de son parc PC tourne sur des OS obsolètes ? Pas de problème, on reste amis mais on signale, on informe, on trace.

9.3 Aller voir un Directeur Général avec des problèmes

Le cas typique, c'est la découverte d'un trou de sécurité majeur sur le SI, qui donne lieu à une longue explication technique au DG, explication qui s'arrête là. Le RSSI qui procède de la sorte à tout faux : il faut certes expliquer, mais présenter un plan d'action chiffré (en JH et en €), une stratégie et au moins une alternative : il faut toujours laisser un choix à un décideur.

9.4 Prendre systématiquement le parti de la DSI

Par exemple, sur un dossier où la technique (SI) et le métier sont en désaccord et où il faut arbitrer entre la sécurité SI et l'ergonomie pour les utilisateurs, le RSSI ne travaille pas pour une MOA ou pour la DSI, il travaille pour l'établissement. Il doit engager les débats vers la recherche d'un compromis. Il y a toujours des solutions, plus ou moins conformes côté SI et plus ou moins ergonomiques côté métier. Toujours.

9.5 Croire tout ce que l'on vous raconte

La DSI vous dit que l'AD est totalement sécure ? Elle vous ment. La MOA vous dit que les procédures dégradées sont à jour ? Mensonge. L'ingénieur système vous affirme que les OS des serveurs sont à jours ? Balivernes. L'ingénieur réseau vous dit que les VLAN sont filtrés ? Bullshit.

Par défaut, toutes les affirmations que l'on vous sort sont fausses tant que vous ne les avez pas vérifiées, soit vous-même soit à partir d'une preuve documentée. La plupart du temps ce sont des mensonges de bonne foi ou par omission, parfois des tentatives de vous intoxiquer. Mais tout le monde ment. Absolument tout le monde.

9.6 Croire que la technique va vous résoudre les problèmes de sécurité SI

La plupart des problèmes ont une origine process, et pas technique. On ne les règle donc pas en mettant encore plus de technique.

9.7 Croire que la prochaine version du machinware va régler tous les bugs

Je n'argumente même plus.

10. Les situations délicates

Il existe des situations où le manuel ne suffit pas forcément.

10.1 La gestion des VIP

C'est le propre des VIP que de réclamer un traitement spécifique : si on n'y prend garde, au final leurs demandes passent par le canal hiérarchique en mode injonction et la sécurité se dégrade sans que le RSSI n'y puisse rien. Être pro actif, pédagogue et chercher des solutions, mêmes imparfaites, est le meilleur moyen de ne pas se retrouver dans cette situation.

Le triptyque des VIP
Cela tourne généralement entre la mise en réseau de leur MAC, la synchronisation messagerie de leur dernier téléphone portable reçu à Noël et la synchronisation Dropbox / Google Drive.

10.2 La gestion des personnes difficiles

Je fais référence aux grincheux, aux mal lunés, à ceux pour qui cela ne va jamais assez, jamais assez vite et pour qui le reste du monde devrait être à leur service exclusif : se voir imposer, en plus, des contraintes de SSI relève à leurs yeux au mieux du crime de lèse-majesté, au pire de la pendaison suivie d'un écartèlement en place de Grève (ou l'inverse) du malheureux.

Il n'y a que deux règles à respecter avec ce genre de personnages, en plus de la même proactivité que pour les VIP :

- rester factuel, ne mettre aucun affect dans les échanges ;
- couper toute discussion dès que le ton devient agressif, les échanges insultants, etc. ; et dans ce cas remonter cela à la hiérarchie.

Les grincheux finissent toujours sur le banc au fond de la cours
D'expérience ces personnages sont assez rares. Il y a des femmes, des hommes, et les informaticiens ne sont pas épargnés, ne leur en déplaise. Ils n'enquiquinent pas seulement le RSSI : ils enquiquinent joyeusement tout le monde, y compris leurs collègues, confrères, subordonnés, etc. Et ils finissent presque toujours par se mettre eux-mêmes au banc du groupe.

10.3 Les profils de savant fou

Il s'agit du gars qui a 200 idées par minutes, la plupart totalement infaisables en termes d'industrialisation et encore plus de réglementaire ou de SSI. Souvent il s'agit d'une personne qui développe à fond du code logiciel sur son temps personnel et qui est persuadé de rendre service à l'Organisation en déployant en douce un logiciel écrit sous ACCESS (ou PARADOX, ou 4D) pour gérer les blocs opératoires, le flux critique de médicaments ou les patients ultra sensibles.

Paradoxalement ils sont bien plus dangereux que les grincheux ci-dessus (pour ces derniers, les demandes excèdent rarement l'informatique personnelle) : vous fermez une porte et ils passent par la fenêtre, et il faut continuellement les garder sous surveillance.

Cloud et savants fous

Avec le Cloud, ils n'ont même plus besoin de la DSI pour mettre à disposition des serveurs ou des partages de fichiers, et vous découvrez un beau matin que le bonhomme (ce sont quasiment toujours des hommes) a développé et fait tourner un système de gestion critique avec des rappels SMS à tout-va et des données ultra sensibles en clair, le tout hébergé sur un serveur en Roumanie.

Seul le réglementaire (RGPD entre autres) brandi sous le nez de leur chef permet de calmer les ardeurs des personnes en question. Tracer par mail le fait que l'institution se dégage de toute responsabilité et que la responsabilité intuitu personae civile et pénale du chef de service est engagée, en général cela fait bouger les lignes.

10.4 La gestion de crise

Il n'existe pas de manuel pour une gestion de crise, puisque la crise est justement ce pour quoi il n'existe pas de manuel[3].

Les REX des entreprises qui ont subi des crises IT majeures font ressortir que c'est justement pendant les temps de crise que les personnalités se révèlent : le timide du fond du couloir s'avère d'une impassibilité salutaire - un vrai pilier pour le reste de l'équipe -, alors que le fort en gueule se délite totalement. Il n'y a pas de règles, certains sont plus aptes que d'autres à gérer ce genre de situation et ce n'est pas un jugement de valeur.

Les entraînements sont nécessaires mais ont leurs limites inhérentes. Les exercices formels permettent de détecter des problèmes techniques (documentation inaccessible, SPOF, etc.) et organisationnels (connaissance non partagée d'une architecture, etc.) mais en aucun cas de reproduire le niveau de stress d'une vraie crise.

3 Cette définition fait débat ; Il en existe d'autre mais je trouve que c'est la plus représentative des situations que j'ai pu vivre.

LA GOUVERNANCE DES DONNÉES

Par Philippe LOUDENOT, Membre d'honneur de l'APSSIS et Cyber Security Strategist - BlueFiles

Approche métier : Point de vue de Philippe LOUDENOT

1. Approche Data

Les organisations, qu'elles soient publiques ou privées, ont entamé depuis de nombreuses années la mise à profit des avantages apportés par les nouvelles technologies. Cependant, force est de constater que cela est souvent réalisé avec une vision exclusivement technique, à reproduire à l'identique ce qui était traité « manuellement » sans toutefois mettre en place les mesures permettant d'assurer la confiance à l'égard des chaînes de valeur des données ; notamment de leur partage et de l'accès à celles-ci. Leur exposition peut poser de graves dangers pour une organisation ou un individu. Face aux risques de fuites et aux menaces de cybersécurité, la protection des données est plus importante que jamais.

2. La mise en place d'une stratégie de gouvernance des données.

Une telle orientation peut être faite pour de nombreuses raisons comme, par exemple :

- la volonté d'améliorer la qualité des données de l'entreprise,
- les capacités analytiques grâce à des données plus qualifiées,
- la suppression ou correction de mauvaises données (doublons, incomplètes),
- améliorer la compréhension des données,
- se mettre en conformité réglementaire, etc.

Cependant, le principal obstacle auquel la plupart des organisations sont confrontées lorsqu'elles entreprennent leur virage numérique n'est pas de nature technique ; il s'agit plutôt de préserver la confiance à l'égard des chaînes de valeur des données. Il faut faire preuve d'une grande confiance pour permettre le partage de ses données et leur utilisation par des tiers qui se trouvent à l'extérieur de la sphère de contrôle.

Pour réellement protéger des données, il faut des règles régissant cette protection. Cette réglementation doit être connue de tous les collaborateurs et tous doivent savoir qu'elle existe. Il faut que celle-ci soit expliquée aux équipes et que les

bonnes pratiques pour la respecter soient partagées. L'outillage mis à disposition des utilisateurs se doit d'être simple et ne pas remettre en cause les habitudes de travail. Un écosystème de partage des données bien rodé est un outil essentiel qui aidera votre organisation à prendre le virage numérique tout en préservant la confiance.

Aujourd'hui les modalités d'échange avec les professionnels de santé se multiplient : nous communiquons par applications de télémédecine, par téléphone, par mail. Toutefois, si l'on peut penser que le développement des échanges dématérialisés peut sembler corrélé à celui des nouvelles technologies, rien n'est moins vrai : cette pratique existe en effet depuis l'Antiquité ; d'après Joël Coste, directeur d'études d'Histoire de la médecine à l'EPHE : «La consultation épistolaire est déjà attestée à l'époque romaine : par exemple, Sénèque y fait allusion dans une lettre destinée à Lucilius». C'est bien plus tard, au 18e siècle, que la pratique se développe jusqu'à devenir un mode de consultation à part entière.

Il est cependant étonnant de s'apercevoir qu'un échange épistolaire du 18ème est mieux protégé que les échanges mail d'aujourd'hui : Si un courrier est mis sous plis et envoyé ainsi protégé à son destinataire, l'email, quand à lui, est disponible à la lecture de tous, comme une carte postale l'est pour le facteur ! Ce moyen de communication presque instantanée est utilisé pour des échanges de santé/patient (ou famille, accompagnant) avec des informations confidentielles sans pour autant que celles-ci soient chiffrées. Et pourtant la protection des données est une obligation légale si les données sont à caractère personnel. Sur l'ensemble de la chaîne de traitement d'un mail entre tous les serveurs intermédiaires, n'importe quelle personne malveillante est en capacité d'intercepter le contenu de ces échanges, et, sans penser systématiquement à malveillance, une erreur peut mettre en visibilité la teneur des échanges.

Il en est de même lors des échanges nécessaires pour le fonctionnement d'une structure de santé. Beaucoup de données doivent ainsi faire l'objet de précautions et de protections : quelles soient stratégiques, financières, de recherches, de rapports, etc. autant de données qui présentent de forts enjeux. Ainsi les données de santé, éminemment sensibles, et pour lesquelles le RGPD impose leur nécessaire protection ne sont pas les seules au sein d'une structure de santé ou médico-sociale à devoir être sécurisées. Les données « ressources humaines », les rapports financiers, de surveillance et de contrôles sont autant de données sensibles, qu'il convient de protéger, notamment lors des transferts et échanges par messagerie. Il convient de respecter le « besoin d'en connaître ». A titre d'exemples, quelques sujets pour lesquels avez-vous mis en place des mesures particulières concernant les échanges de données dans le cadre :

- de la certification des comptes,
- de la réception de documents en provenance de patients, de leurs famille ou accompagnant,
- des échanges avec différents fournisseurs, collectivités…

3. Comment mesurer la sensibilité des données

Une information sensible est une donnée nécessitant une protection contre l'accès non autorisé, afin de préserver la sécurité d'un individu ou d'une organisation.

Les informations sensibles se distinguent des informations publiques, car elles ne peuvent pas être consultées à partir d'un dossier sans restriction. Ainsi, l'exposition de ces données sensibles peut avoir des conséquences néfastes pour la confidentialité d'une personne ou les finances d'une organisation. Afin de déterminer comment traiter les données, il est important de pouvoir mesurer leur sensibilité. Pour ce faire, on peut se baser sur la confidentialité, l'intégrité et la disponibilité des données. Il faut aussi considérer l'impact qu'aurait l'exposition de ces informations sur une structure.

Cette façon de mesurer la sensibilité des données est recommandée dans le guide du Federal Information Processing Stanrdards (FIPS) élaboré par le National Institute of Standards and Technology (NIST).

La confidentialité est liée à la vie privée. Les entreprises peuvent mettre en place des mesures pour empêcher l'accès non autorisé aux données sensibles, tout en y permettant l'accès pour les personnes autorisées. Il s'agit d'une simple formation fondamentale, permettant à tous les employés de saisir les risques de sécurité liés au traitement d'informations et de découvrir les techniques permettant de les protéger. Pour renforcer la confidentialité, on peut citer le chiffrement de données, les mots de passe, l'authentification à deux facteurs, la vérification biométrique ou les jetons de sécurité.

Il est préférable de limiter l'exposition et les transferts des données au strict minimum et en utilisant les moyens permettant de garantir le besoin d'en connaître.

L'intégrité des données désigne leur cohérence, leur exactitude et leur fiabilité tout au long du cycle de vie. Les données sensibles ne doivent pas pouvoir être modifiées pendant un transfert, et ne devraient pas pouvoir être altérées par des personnes non autorisées en cas de fuite de données.

Enfin, la disponibilité consiste à s'assurer que toutes les informations sensibles et systèmes informatiques restent accessibles.

4. Les conséquences d'une fuite de données ?

L'utilisation illégitime de vos données : Bien évidemment, le premier risque en cas de fuite de données, c'est l'utilisation illégitime de ces informations. Il devient ainsi difficile (voire même impossible) de contrôler ces situations. Une telle usurpation peut avoir de lourdes conséquences.

Les amendes imposées par les autorités : Le RGPD impose aux professionnels des règles strictes concernant la sauvegarde et l'utilisation de données personnelles. En cas d'utilisation « hasardeuse », une amende définie à 4% du chiffre d'affaires de l'entreprise concernée est appliquée. Et ce montant peut être multiplié suivant certaines situations.

Une perte de temps : Outre les impacts financiers, une fuite de données engendre bien souvent des pertes de temps considérables. En effet, ce type de situations peut bouleverser rapidement l'organisation d'une entreprise ou société.

La médiatisation : L'impact négatif généré par une médiatisation concernant une fuite de données entraine une dégradation de l'image de marque mais également une perte de confiance qui sera très difficile à regagner.

La perte de données peut paralyser une structure : Les fuites de données entraînent parfois des pertes d'informations capables de paralyser les activités d'une entreprise ou société. Généralement, ces situations précèdent des tentatives de ransomwares (récupération de fichiers suite à un paiement par crypto-monnaies).

5. 5 conseils pour éviter la fuite ou le vol de données

Pour éviter les effets négatifs d'une perte massive d'informations sensibles d'une organisation, il est judicieux de mettre en œuvre des stratégies à dimension technologique et humaine :

- connaître avec précision les informations qui nécessitent le plus de protection que ce soit pour l'intérêt de l'organisme ou parce que la réglementation l'impose (ex RGPD),
- créer une politique de sécurité des données en prenant en compte les besoins métiers propres et les moyens les plus efficaces pour sécuriser les données, tout en respectant le bon équilibre en risque et productivité,
- sensibiliser les collaborateurs, anciens comme nouveaux, par rapport aux bonnes pratiques de manipulation des données et particulièrement leurs échanges,
- adopter le chiffrement des données particulièrement durant leur transfert. Proposer et mettre en œuvre des solutions de confiance !

Pour simplifier, on peut dire que la gouvernance des données consiste à savoir où se trouvent vos données, comment elles sont utilisées et si elles sont bien protégées, particulièrement lors de leurs envois ou transferts. Une bonne gouvernance garantit outre l'intégrité et la cohérence des données, mais empêche aussi qu'elles soient utilisées ou manipulées à mauvais escient.

11. POUR ALLER PLUS LOIN

11.1 Évolutions à venir du métier

Il y a 10 ans à peine, dans pas mal de secteurs et entreprises, le RSSI était celui qui gérait l'antivirus ou le pare-feu (cf. les types de RSSI, plus haut). Dans les entreprises les plus matures, le RSSI est un gestionnaire de risques qui se concentre sur ses fonctions d'audit et de contrôle, de premier ou second niveau.

La fonction de RSSI est mature dans une entreprise lorsque ce dernier passe entre 50 % et 75 % de son temps à auditer, le reste à se faire auditer (conformités aux différentes normes ISO auxquelles sont soumis l'entreprise).

Selon que ce volet conformité va devenir ou pas juridiquement ou commercialement coercitif (l'entreprise est soumise à la certification des comptes, qu'elle le veuille ou non, mais garde encore une marge de manœuvre pour ce qui est d'autres normes, mais pour combien de temps encore ?), la fonction RSSI a de bonne chance d'évoluer vers un département de Conformité.

Comme à chaque mutation majeure dans l'entreprise, il y a compétition pour déterminer qui des différents profils tiendra la dragée haute aux autres et dirigera, de façon formelle ou informelle. Dans les années 50 et 60, les entreprises de techno type France Telecom ou des entreprises du secteur de la Défense étaient, de fait, pilotées par des ingénieurs. On assistait même à des formations de baronnies informelles - telle école d'ingénieur noyautait telle entreprise, on pense par exemple aux Mines ou aux Arts et Métiers. Dans les années 80 et 90, le pouvoir s'est déplacé des ingénieurs vers les financiers, et ce sont les HEC et consort qui ont dirigé de facto la plupart des grandes entreprises, tout du moins en France.

Il y a de fortes chances pour que le centre de gravité, qui se déplace constamment, arrive - ou revienne selon le point de vue - vers les technocrates purs que sont les normalisateurs, les « éditeurs de règles internes » comme les appelle Pierre-Yves Gomez. Le pouvoir risque de revenir vers les qualiticiens, les juristes, le DPO et le RSSI. Si vous n'en êtes pas convaincus, sachez que le DPO est une des rares personnes dans l'entreprise qui a le pouvoir virtuel de stopper un projet (les conseils et alertes qu'il prodigue sont difficiles à passer sous silence au bout d'un moment) et ce, sans disposer d'aucun pouvoir hiérarchique.

La place et la tour

C'est sous ce titre que Niall Ferguson, un des plus prolixes historiens actuel, analyse l'Histoire depuis l'aube du XVIIIème siècle, selon un angle de vue pour le moins surprenant : la compétition constante entre la hiérarchie (la tour) et les réseaux (la place). Le réglementaire (notamment le RGPD) est dans une certaine mesure le retour du réseau face à la hiérarchie.

Que le RSSI et le DPO rejoignent donc à terme un département Conformité / Contrôle-audit interne ne fait plus de doute. L'évolution des deux métiers vers du juridique et du contrôle, dans les deux

cas, peut laisser à penser que leur raison d'être est de fusionner. On va alors assister à la naissance d'un processus extrêmement puissant au sein des entreprises, il n'est d'ailleurs même pas certain que la Qualité leur reste longtemps rattachée.

Après, le propre des prévisions est d'évoluer constamment, et il y a ne serait-ce que 5 ans je n'aurais pas écrit les mêmes lignes. La boule de cristal n'existe pas encore, qui me permettra de prédire sans risque d'erreur les 5 prochaines années.

11.2 Connaissances annexes indispensables

Certaines connaissances non techniques peuvent être d'une grande utilité pour comprendre et interpréter le comportement des personnes, des services, des groupes d'utilisateurs. L'exemple le plus connu est l'ingénierie sociale, qui est à la base d'un bon nombre d'attaques telles la fraude au Président ou les phishings sur Internet.

Il est utile, pour un RSSI, de connaître à minima :

• le concept de la pyramide de Maslow qui traite de l'échelle des besoins ;
• l'expérience de Asch qui met en évidence les comportements de conformité ;
• toute la théorie des biais de décision, dont un des meilleurs spécialistes français est Olivier Sibony ;
• les bases de la négociation ;
• les bases de la PNL (Programmation Neuro Linguistique) ;
• les bases de la socio dynamique ou autre méthode d'analyse comportementale ;

Dit autrement, les « soft skills » font partie intégrante du bagage indispensable du RSSI intergalactique / tout terrain : se focaliser uniquement sur les compétences techniques est un mauvais choix sur le long terme.

12. ANNEXE 1 : LES 10 COMMANDEMENTS

Commandement n°1 : tout le monde vous ment

Commandement n°2 : consacrer au moins 25 % de son temps à de la veille technologique, juridique et réglementaire

Commandement n°3 : se souvenir que les incidents sur le SI sont autant causés par des dysfonctionnements organisationnels que par des soucis techniques

Commandement n°4 : rester en conseil, alerte et audit, la MOA est seule propriétaire de ses risques

Commandement n°5 : audits et contrôles sont les meilleurs amis du RSSI

Commandement n°6 : adapter son discours à son auditoire

Commandement n°7 : la négociation est plus efficace sur le long terme que le passage en force, les ennemis coûtent trop cher au RSSI

Commandement n°8 : le RSSI dispose de la meilleure fenêtre de tir pour faire avancer ses projets après un crash

Commandement n°9 : avant d'acheter des logiciels payants et chers, bien s'assurer que l'on est arrivé au bout du potentiel d'un simple traitement de texte et des outils en Open Source

Commandement n° 10 : si vous croyez avoir une idée ou un problème, quelqu'un les a forcément eus avant vous ; même cette idée je l'ai piquée à quelqu'un d'autre

Bonus 1, proverbe chinois : les tuiles des toits ont toutes été posées par temps sec

Bonus 2, autre proverbe chinois : quand tu ne sais pas quoi dire, cite un proverbe chinois

13. ANNEXE 2 : BIBLIOGRAPHIE

13.1 Management de la sécurité des systèmes d'information

« La sécurité du système d'information des établissements de santé », Cédric CARTAU, Presses de l'EHESP, 2ème édition
« Management de la sécurité de l'information », Alexandre FERNANDEZ-TORO, Eyrolles

13.2 Ouvrages techniques

« Résistez aux hakers », Cédric BERTRAND, Vuibert
A télécharger sur le site de l'APSSIS, les ouvrages sur la cyber résilience
Opus 1 : la gestion des mots de passe
Opus 2 : les cyber attaques
Opus 3 : les habilitations d'accès aux données
Opus 4 : la sécurisation du Cloud
Opus 5 : les indicateurs

13.3 Ouvrages généralistes sur la gestion des risques

« Peut-on vivre sans risque », Jean-Marc CAVEDON
« Obfuscation », Helen NISSENBAUM, C&F éditions
« La gestion des risques », Olivier HASSID, Dunod

13.4 Ouvrages sur la sociologie du traitement des risques

« Les décisions absurdes. Sociologie des erreurs radicales et persistantes », Christian MOREL, Paris, Gallimard, coll. « Bibliothèque des sciences humaines », 2002.
« L'inquiétant principe de précaution », Gérald BRONNER
« Vous allez commettre une terrible erreur », Olivier SIBONY

13.5 Soft skills

« Saint Germain ou la négociation », Francis WALDER
« Comment réussir une négociation », Roger FISHER, Bruce PATTON
« Négocier avec des gens difficiles », Roger FISHER, Bruce PATTON

14. ANNEXE 3 : RESSOURCES DOCUMENTAIRES

14.1 Revues

http://www.dsih.fr avec le formulaire d'abonnement

14.2 Sites institutionnels

http://www.ssi.gouv.fr/
http://www.metiers-fonctionpubliquehospitaliere.sante.gouv.fr
http://signalement.social-sante.gouv.fr
http://cyberveille-sante.gouv.fr
http://cybermalveillance.gouv.fr

14.3 Sécurité des systèmes d'information

http://www.apssis.fr/

14.4 Blogs

http://www.volle.com
http://www.laurentbloch.org/fr/
http://sehiaud.blogspirit.com/
http://vblog.io
http://korben.info/n-guide-hygiene-informatique-particulier.html

14.5 Droit

http://www.hospidroit.net/

14.6 Dépôt de preuve numérique

http://www.mapreuve.fr/

14.7 Sites de formation

http://www.internetsanscrainte.fr
https://www.cybersimpel.be/fr
Le MOOC de l'ANSSI, une référence : https://secnumacademie.gouv.fr
Le MOOC de la CNIL : https://atelier-rgpd.cnil.fr/login/index.php
Un outil de formation, aussi bien pour les sysadmin que les utilisateurs : https://sudo.pagerduty.com
MOOC Vigipirate : https://vigipirate.gouv.fr/

14.8 Outils de sensibilisation

Un petit outil sympa d'auto évaluation de ses propres objectifs personnels de sécurité : https://securityplanner.org
Un outil de sensibilisation au phishing : https://phishingquiz.withgoogle.com

14.9 Chaines Youtube spécialisées

Micode : https://www.youtube.com/channel/UCYnvxJ-PKiGXo_tYXpWAC-w
Paf le Geek : https://www.youtube.com/channel/UCCSHWqosFfYJY5v2WqbTLhg

14.10 10 Vidéos sur la SSI

14.10.1 Clip Airbus

https://www.youtube.com/watch?v=yBL4eco0NCs
https://www.youtube.com/watch?v=kiw4B00iJzs
https://www.youtube.com/watch?v=kiw4B00iJzs

14.10.2 Divers

Vidéo sur l'ingénierie en ligne : https://www.youtube.com/watch?v=79uD8mX7oeM
Nothing To Hide : https://vimeo.com/193515863
Festival du film sur la SSI : https://portail-ie.fr/short/1486/1ere-edition-du-festival-du-film-securite-le-palmares-en-videos

14.10.3 RGPD

Le RGPD expliqué par la CNIL dans une vidéo youtube : https://www.youtube.com/watch?time_continue=77&v=OUMGp3HHel4

14.11 Ressources documentaires

MindMapping sur les concepts SSI : https://www.amanhardikar.com/mindmaps.html
Guide de la CNIL pour chiffrer ses documents : https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires
Kit de sensibilisation : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/kit-de-communication
Vue d'ensemble des malwares : https://docs.google.com/spreadsheets/d/e/2PACX-1vRCVzG9JCzak3hNqqrVCTQQIzH0ty77BWiLEbDu-q9oxkhAamqnlYgtQ4gF85pF6j6g3GmQxivuvO1U/pubhtml#
Quick Wins pour les RSSI : https://goupilland.net/articles/quickwins-rssi/
La boite à outils ANSSI : https://www.ssi.gouv.fr/agence/cybersecurite/cybermois-2019/la-boite-a-outils/

14.12 Serious Game

http://targetedattacks.trendmicro.com

14.13 Podcast

https://www.comptoirsecu.fr/

14.14 Fiches métier SSI

Annuaire des métiers du CIGREF, version 2021
https://www.cigref.fr/wp/wp-content/uploads/2021/12/Cigref-Nomenclature-RH-des-profils-metiers-du-SI-version-intermediaire-2021.pdf
Répertoire des métiers de la FPH
https://metiers-fonctionpubliquehospitaliere.sante.gouv.fr
Métiers de la cyber, panorama de l'ANSSI :
https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/

15. ANNEXE 4 : LES OUTILS

Ne sont listés que les outils gratuits ou ceux qui offrent une version non limitée dans le temps (mais qui peut être bridée dans les fonctionnalités).

15.1 Mot de passe

Coffre fort : https://keepass.info/
Calcul de force / complexité de mot de passe : https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

15.2 Boites aux lettres

Adresse mail jetable : http://www.yopmail.com/
Boites aux lettres sécurisées : https://protonmail.com/
Messagerie sécurisée : https://www.olvid.io/fr/
Messagerie sécurisée instantanée : https://signal.org/fr/
https://element.io/

15.3 Analyse d'un AD

https://www.pingcastle.com/
https://www.purple-knight.com/

15.4 Détection de compromission d'un compte

HaveIBeenPawned : https://haveibeenpwned.com/
Firefox Monitor : https://monitor.firefox.com/

15.5 Analyse d'une messagerie

Test de la robustesse et conformité d'une messagerie : https://mecsa.jrc.ec.europa.eu
Scan de conformité de serveur de messagerie : https://ssi.economie.gouv.fr
Test d'indésirabilité (spam) de ses mails : https://www.mail-tester.com/

15.6 Solution MFA

Qwerty card : https://www.qwertycards.com/
http://www.passwordcard.org/fr

15.7 Outil d'analyse réseau

Analyse des trames sur un LAN : https://suricata.io/
Scan de réseau domestique avec recherche de vulnérabilité : https://www.bitdefender.com/solutions/home-scanner.html
Nmap : https://nmap.org/zenmap/
Outil domestique : https://www.advanced-ip-scanner.com/fr/

15.8 Protection antivirale

Scanner de Microsoft : https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
Le site de Virus total : www.virustotal.com
Scanner en ligne : https://www.f-secure.com/fr/home/free-tools/online-scanner

15.9 Vérification de compromission ou de réputation d'un site Web

https://global.sitesafety.trendmicro.com/
https://www.urlvoid.com/
https://talosintelligence.com/
https://internet.nl/
https://observatory.mozilla.org/
https://safeweb.norton.com/

Vérification de typo squatting : https://brand-alert.whoisxmlapi.com/api

15.10 Scanners

Scanner d'IoT : https://www.shodan.io/
Contrôle de fonctionnement d'un site Web : https://zonemaster.net/domain_check
Test des MX : https://mxtoolbox.com/
Test de configuration SSL : https://www.ssllabs.com/ssltest/index.html
https://www.hardenize.com/
https://www.purplemet.com/
https://securityscorecard.com/

15.11 Chiffrement

http://www.truecrypt.org/
http://www.axantum.com/AxCrypt/
https://www.mybluefiles.com

15.12 Carte des attaques mondiales en temps réel

https://cybermap.kaspersky.com/fr/stats/

15.13 Anonymisation

http://ipjetable.net/

15.14 Test de phishing

https://phishinsight.trendmicro.com/?v2

15.15 Divers

Calculer le prix de vos données personnelles : https://simulator.drdata.io/
Outil de test de maturité de la sécurité du SI : https://www.zensi.fr/outils/maturite_ssi/mssi-2011.html

15.16 Portails Open Source

http://www.framasoft.org/
http://www.novaforge.org/
http://www.open-source-guide.com/
https://sill.etalab.gouv.fr/software

16. ANNEXE 5 : CE QUE LE DPO N'EST PAS

16.1 DPO, ce que cela n'est pas

Il arrive assez régulièrement que des confrères DPO me contactent pour me signaler certaines de leurs difficultés dans l'exercice de leur mission, et cela tourne régulièrement autour du même sujet : leur responsable de traitement (RT) refuse de mettre en œuvre les préconisations de sécurité dudit DPO, entendre par là les mesures destinant à réduire les risques identifiés. Le confrère en question me demande alors comment contraindre le RT à appliquer les mesures en question. Il me semble qu'il y a là une erreur de positionnement, et cela vaut bien un billet.

Les articles 38 et 39 du RGPD sont tout à fait explicites : le DPO a un rôle de conseil et d'alerte, il ne reçoit pas d'instruction (au sens où personne n'a à lui dicter ses actions) et il est indépendant. Prenons l'exemple d'un traitement qu'un RT voudrait mettre en place : si le RT contourne le DPO (intentionnellement ou pas), c'est clairement contraire à l'article 38-1 qui dit que le DPO doit être associé pour qu'il soit en mesure, justement, de jouer son rôle de conseil et d'alerte. Dans un tel cas, la responsabilité du DPO est totalement dégagée et celle du RT doublement engagée si un contrôle des autorités relevait un manquement au RGPD en plus du fait que le DPO n'a pas été consulté.

L'esprit du RGPD semble être qu'il n'est pas du ressort du DPO que de réaliser une appréciation des risques - il doit plutôt assister le RT dans la réalisation de celle-ci -, même si dans les faits le niveau technique semble plutôt relever des compétences d'un DPO que de celle d'une MOA.

On m'a rapporté un jour le cas d'un RT qui refusait obstinément un risque en particulier dans l'analyse réalisée par le DPO, et qui posait comme condition à la signature du PIA le retrait du risque en question (ce cas semble rare). Si le DPO acceptait de retirer cette ligne de son analyse des risques, il commettrait une erreur : en cas de survenance du risque correspondant justement à cette fameuse ligne et en cas de contrôle de la CNIL, il lui serait reproché de n'avoir pas mentionné ce risque dans son analyse (et à ce moment vous vous doutez bien que les personnes lui ayant demandé de retirer cette ligne seraient subitement atteinte d'une amnésie généralisée, le laissant gros-jean comme devant). La réponse est simple : le DPO ne reçoit pas d'instruction, personne n'a à lui dire quelle analyse il fait de telle ou telle situation, il est seul avec sa conscience dans ce contexte. Le RT peut parfaitement refuser de signer le PIA, mais dans ce cas le DPO doit matérialiser le fait que, tel jour et telle heure, le PIA a été présenté au RT qui a refusé de le signer, et consigner ce dysfonctionnement dans son rapport annuel. Si de plus le risque en question est majeur (ce qui était le cas dans l'exemple cité), en cas de survenance du risque le RT (qui non seulement a voulu mettre le problème sous le tapis, mais en plus n'a rien fait pour le régler) devrait se justifier doublement auprès des autorités de contrôle, le DPO quant à lui serait totalement exempt de reproche. La traçabilité des échanges est très clairement l'assurance-vie

du DPO.

Evidemment, cette position du DPO, confortable par certains aspects, peut être déroutante par d'autres. Un RT pourrait parfaitement valider une appréciation des risques, et pour autant décider de ne prendre aucune des mesures recommandées par le DPO. C'est le problème du RT et de lui seul, et le DPO doit « faire son deuil » de sa capacité à imposer à un RT des décisions qu'il faudrait prendre (selon le DPO) mais pour lesquelles il n'est justement pas décideur : c'est le RT et lui seul qui décide, ou pas, de suivre les recommandation du DPO et il est souverain dans cette décision. Une fois que le DPO s'est bien assuré que son rôle de conseil et d'alerte a été joué, et que le RT a bien compris les risques encourus, ce qui suit n'est pas de son périmètre de décision. Le RT est propriétaire de ses risques, et jusqu'à preuve du contraire ce n'est pas le DPO qui dirige l'entreprise.

Cela peut donner des situations cocasses (et les exemples qui suivent sont bien entendu caricaturaux et ne servent qu'à illustrer le propos de l'article). Imaginons une MOA qui demanderait à son DPO de réaliser la compilation de tous les risques RGPD de l'établissement : le DPO serait en droit de retourner la question et de répondre à sa MOA que c'est lui, le DPO, qui demande à sa MOA un état des lieux des risques RGPD de l'établissements, et qu'il choisit justement ce thème pour son prochain audit RGPD. Inversement, sur un dossier bien tordu dont le DPO voudrait se mêler, la MOA pourrait tout à fait signifier au DPO que ses services ne sont pas requis sur ce dossier, la MOA pourrait d'ailleurs refuser de répondre à la demande d'audit du DPO sur ce traitement (refus que le DPO devra bien entendu consigner dans son rapport annuel). Dans le même registre, si un RT demandait au DPO de réaliser l'analyse des risques d'un traitement, ce dernier pourrait refuser au motif que cela n'est pas dans sa mission, qui se borne éventuellement à fournir une méthode d'analyse de risque documentée et à former le RT sur cette méthode. Le RT pourrait, en contrepartie, refuser de prendre ladite méthode argumentant qu'il a déjà la sienne.

Plus sérieusement, il est important de retenir cette dualité entre celui qui a un rôle de conseil, et celui qui décide et qui est propriétaire de ses actifs (et les risques en font partie). Un DPO dont 100 % des recommandations ne sont pas systématiquement suivies ne doit pas le prendre comme une attaque personnelle, mais simplement comme le fait qu'une MOA fait face à une somme de contraintes multiples (dont le RGPD fait partie mais n'en n'est qu'une composante), que diriger c'est faire des choix et que parfois le choix n'est pas celui d'une conformité à 100 %. Enfin, un DPO qui irait souvent au clash avec ses RT devrait se poser des questions sur sa pratique professionnelle .

Ah, j'allais oublier : RSSI c'est pareil.

16.2 DPO, ce que cela n'est pas - suite

Il n'était pas prévu de faire un second volet, mais à la suite du premier article (ici[1]) et du grand nombre de remarques et commentaires (notamment de Boris MOTYLEWSKI, créateur entre autres de www.cybersecu.fr), il semble important de faire quelques précisions.

Tout d'abord, citant le cas d'un confrère à qui son RT avait demandé de retirer un risque du PIA sous peine de ne pas signer, j'ai écrit que « si le DPO acceptait de retirer cette ligne de son analyse des risques, il commettrait une erreur …/… et en cas de contrôle de la Cnil, il lui serait reproché de n'avoir pas mentionné ce risque dans son analyse ». En toute rigueur, c'est faux : le DPO peut écrire n'importe quoi dans le PIA, au final c'est le RT qui en est responsable.

Dans la pratique, il faut nuancer : la plupart du temps, même si l'analyse des risques est débattue avec le RT, dans les faits c'est bien le DPO qui rédige le PIA - rien d'anormal à cela si cela se borne à mettre en forme avec des modèles prédéfinis ce que le RT a validé. Sauf que, dans le cas cité d'un risque que le RT refuse, si le DPO en reste là (pas de matérialisation de ce risque dans le PIA), en cas d'incident le RT aura beau jeu d'argumenter de sa non-expertise et du défaut de conseil de son DPO. Certes le DPO n'a qu'un rôle de conseil et d'alerte, mais en même temps c'est lui qui est supposé détenir l'expertise, et en droit français la position d'expert est très inconfortable si l'on n'est pas capable de prouver que l'on a bien alerté sa MOA. Il n'y a, à ma connaissance sur le RGPD, pas de jurisprudence sur ce cas pas si tordu que cela, mais personnellement je ne me risquerais pas à jouer avec les allumettes d'un PIA incomplet : en tant que DPO, je préfère être dans la situation d'un PIA complet et non signé (avec traçabilité de la présentation au RT) que de parier sur le strict rôle de conseil et d'alerte supposé protéger un DPO. Cela étant, ce n'est qu'un avis.

A partir de là se posent deux questions : comment un DPO peut-il faire connaître aux MOA que sa présence est nécessaire sur l'analyse RGPD des traitements mis en œuvre, et comment peut-il habilement jouer avec une carotte et un bâton que la réglementation de lui accorde pas.

Sur la première question, le DPO doit bien entendu se faire connaître de tous, et ceci par tous les canaux à sa disposition. Réunions de service, de pôle, comité machin, coproj bidule, lettre d'information dans le bulletin de salaire, journal interne, etc. A minima, la DSI, les directions techniques, les directions de RetD, les directions achats, opérationnelles, les comités directeurs doivent être adressés par une communication DPO, même rudimentaire. Cela étant, il est matériellement impossible de s'assurer qu'aucun traitement ne sera mis en œuvre sans que le DPO soit sollicité, et sur ce coup on ne pourrait pas lui reprocher grand-chose. Une des mesures simples que le DPO peut mettre facilement en œuvre, c'est de rendre facilement accessible dans tout l'établissement son registre des traitements (ou en tout cas une version édulcorée), comme cela chacun peut vérifier que son traitement est bien dans la liste et alerter le DPO si besoin.

Sur la seconde question, il y a clairement trois types de DPO :

• celui qui tente par tous les moyens d'imposer au RT les mesures de réductions des risques issues de l'analyse des risques ; nous avons vu dans le premier article que ce positionnement est non seulement contraire à l'esprit du RGPD, mais en plus constituerait un dysfonctionnement dans la chaîne de commandement, cela voudrait dire en effet que c'est le DPO qui dirige la boite ;
• celui qui se retranche derrière les textes, rien que les textes et seulement les textes : « j'ai joué mon rôle de conseil et d'alerte, vous ne suivez pas mes préconisations, je le note dans mon rapport annuel et basta » ; ce genre de de positionnement constitue la version d'entrée de gamme du DPO ;
• la vision intermédiaire, que je préconise, voir ci-après.

Cette vision consiste, pour le DPO, à user autant que possible des textes, à la fois dans la lettre et dans l'esprit, pour amener subtilement les RT (et surtout les fournisseurs) à réduire les risques, sachant qu'il va exister un point au-delà duquel le DPO n'a plus la main ni de moyen de négociation - en gros, dès que cela va coûter trop cher. Clairement ce positionnement va au-delà de l'esprit du RGPD (pour lequel le DPO a essentiellement un rôle de conseil et d'observateur, pas d'acteur), mais personnellement j'ai cette vision duale du rôle de DPO, dont la seule valeur ajoutée au sein de l'entreprise ne peut pas (selon moi) se borner à de l'audit interne. On est clairement à la frontière de l'intrusif, mais une bonne méthode consiste à poser des questions (c'est comme cela que faisait Socrate, il faut juste ne pas finir comme lui) du genre : « cher RT, comment comptez-vous réduire ce risque que vous avez-vous-même estimé majeur ? » (je n'ai encore jamais connu un RT qui mette la tête dans le sable devant une telle question).

Mais le vrai challenge d'un DPO, c'est de poser les questions poil à gratter, le truc qui pique les yeux, enfin vous voyez de quoi je parle…et de rester copain avec son RT. Accessoirement, cela permet de ne plus déjeuner tout seul à la cantoche.

Ah, j'allais oublier : RSSI c'est pareil.

1 https://www.dsih.fr/article/3578/ce-que-le-dpo-n-est-pas.html?&utm_medium=email&utm_source=nl&utm_campaign=NL316

APSSIS

Association Pour la Sécurité des SI de Santé

84 rue du Luart
72160 Duneau

06 29 36 59 95

secretaire@apssis.com

www.apssis.com

Création graphique : Corvy-Graphisme - Crédit photo : Freepik