



**Menaces informatiques et
Pratiques de sécurité en France
Édition 2018**

Les établissements de santé de + de 100 lits

Stéphane MONEGER

Responsable Système d'Information



Présentation de l'échantillon

© Périmètre d'étude modifié :

- établissements de 100 lits et plus,
- Activités hospitalières et d'Hébergement Médicalisé

© 127 hôpitaux et 24 structures d'hébergement médicalisé ont répondu :

- 67% appartiennent à un groupement
- Responsable sécurité SI ou , ou à défaut RI ciblés

© Des résultats redressés pour obtenir des chiffres représentatifs :

- types d'établissements (Activités hospitalières / Hébergement médicalisé)
- des tranches en nombre de lits

Le « boom » des formalisations de PSSI

- © Croissance spectaculaire du nombre d'établissements ayant formalisé leur PSSI : de 50% à 92% en 4 ans (Ces politiques sont largement diffusées, souvent à jour et massivement soutenues par la DG)



- © Les principaux acteurs sont la DG, la DSI, et le RSSI.
- © 84% des établissements pilotent leur Sécurité de l'Information en s'appuyant sur des normes et référentiels



Une croissance forte de la fonction RSSI



© Fonction RSSI attribuée dans 80% des établissements



© Fonction a temps plein dans 1 établissement sur 2



© Une « équipe » SSI dans 70% des établissements



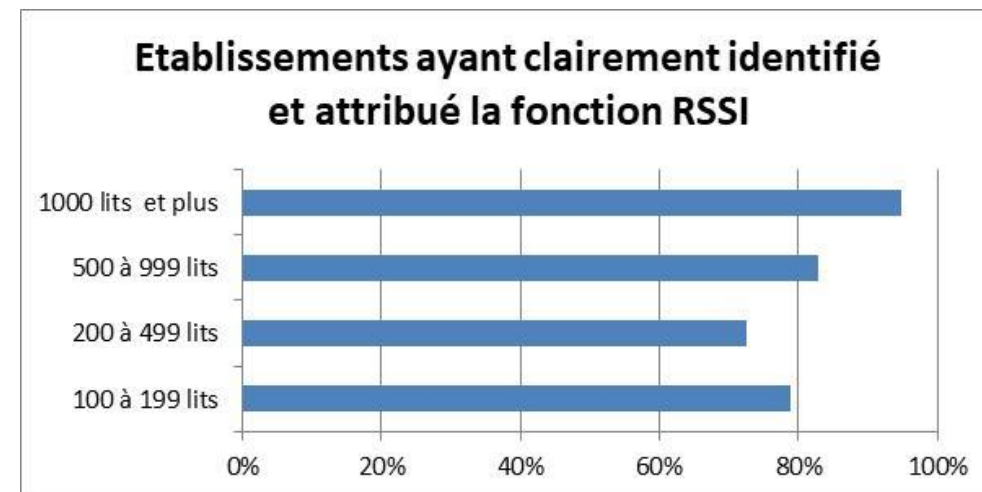
© Des coûts liés à la sécurité mal évalués dans plus de 81% des établissements.



© Un budget sécurité en augmentation pour plus d'un établissement sur 3 ..



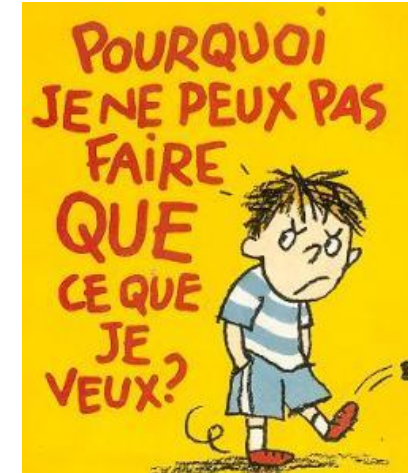
© Manque de budget et absence de personnel qualifié sont les principaux freins.



Sécurité des ressources humaines



- © Tous les établissements ont un charte d'utilisation du SI largement diffusée
- © 80% des **établissements** disposent d'une procédure de gestion des départs
- © Une politique de sensibilisation à la sécurité de l'information en croissance : 3 établissements sur 5 ont un programme





Inventaire des Actifs

- © Très forte progression de l'inventaire des actifs qui est quasiment généralisé (90% des répondants)
- © La classification au moins partielle des actifs progresse, pour atteindre en moyenne 71 %









Analyse des Risques

- © L'inventaire, au moins partiel des risques devient une généralité (81% des répondants) mais 1/3 des établissements seulement a réalisé une évaluation formelle avec une méthode (EBIOS, ISO 27005, MEHARI)
- © Cette évaluation est menée principalement par le RSSI (56% des cas) ou le RI/DSI (21%)
- © Un plan d'amélioration de la sécurité dans 3 établissements sur 4



Contrôle d'accès : 5 approches de sécurisation logique



-  Habilitation basés sur des rôles et profils (de 64% à 82%)
-  Authentification forte par « calculatrice » à mot de passe non-rejouable (de 10% à 31%)
-  Workflows d'approbation des habilitations (de 31% à 48%)
-  Provisionning automatique de comptes et droits (de 28% à 42%)
-  Sigle Sign On (de 34% à 41%)
-  Baisse significative de l'usage de carte CPS (de 67% à 53%)

L'utilisation de différentes technologies n'est pas homogène et varie selon la taille des structures de santé.

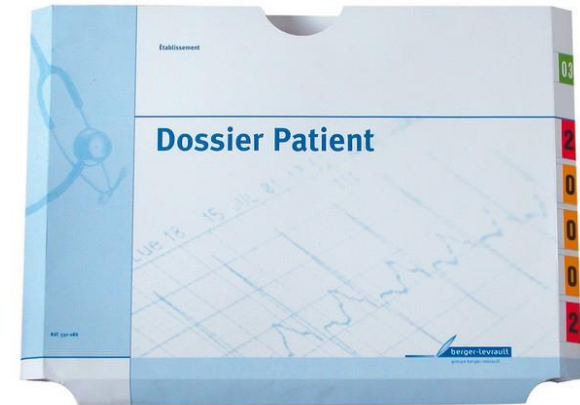
 70% des établissements disposent de **procédures formelle de Gestion des Comptes** (user et admin). En augmentation depuis 2010

 87% des établissements disposent de règles de **constitution et de péremption des mots de passe** pour tous les accès

Sécurité physique et environnementale



© La sécurité physique des dossiers des patients papier de plus en plus sous la responsabilité du corps médical.





© 3 dispositifs majeurs de sécurisation physique des salles machine :

- la détection incendie
- La vidéo-surveillance
- Le contrôle d'accès par badge






Sécurité liée à l'exploitation

Technologies et approches de sécurisation :

-  En 4 ans, une nette priorité à la **protection des outils de mobilité** (Outils de chiffrement, Pare-feu, antivirus)
-  Une croissance forte des **sondes** : détection IDS et prévention IPS

Gestion des vulnérabilités techniques :

-  Près de 9 établissements sur 10 réalisent des **veilles permanentes** en vulnérabilités et en solutions de sécurité de l'information.
-  1 sur 2 formalise des procédures de **déploiement de correctifs** de sécurité.
-  Manque de connaissance du périmètre concerné notamment en ce qui concerne le biomédical et les services techniques.

Sécurité des communications :

Evolutions dans les pratiques de sécurité



© Un filtrage systématique des accès Web dans 75% des établissements contre 14% en 2014



© L'interdiction du BYOD reste stable (77% des établissements).

© L'interdiction des Réseaux Sociaux reste stable (44% des établissements).



© Accès au SI depuis des postes extérieurs non maîtrisés interdit dans plus d'1 établissement sur 2 mais en recul.

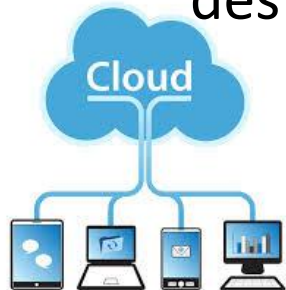
© L'interdiction des smartphone/tablette d'entreprise diminue : un peu moins d'1 établissement sur 2

© Un recours à des spécialistes de l'hébergement de données de santé relativement répandu :









- 42% des établissements ont externalisé tout ou partie de leur SI
- 6% ont externalisé leur SI en totalité
- La moitié des établissements effectue un suivi régulier de l'hébergeur à l'aide d'indicateurs de sécurité
- 30% des établissements réalisent des audits de leurs hébergeurs

© Dans 25% des établissements, les utilisateurs ont recours à des services en Cloud :



- Privé à 49% sinon public ou hybride
- Sous contrôle de la DSI (74%)
- Faiblement règlement en interne « politique d'utilisation du cloud »

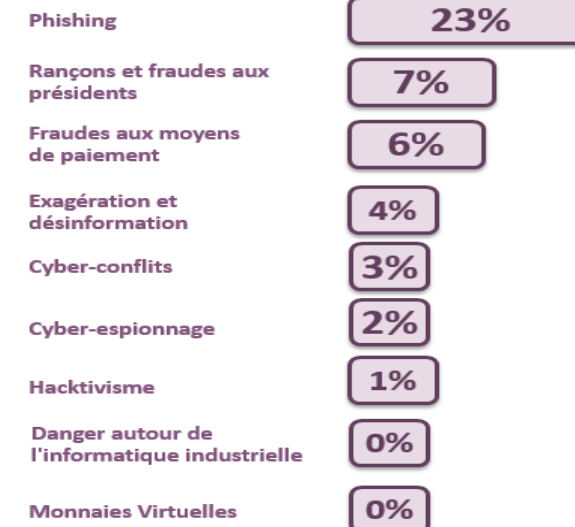
Gestion des incidents

-  © 57 % des établissements ont une cellule de collecte et de traitement des incidents.
-  © pas d'évolution quant aux principales sources d'incidents
-  © 75% des incidents sont résolus en moins de 24h
-  © recul global de la sinistralité - Typologie des incidents :
 - © #1 : indisponibilité suite à des pannes d'origine interne
 - © #2 : plus de 42% des établissements déclarent des infections par virus
 - © #3 : autres « attaques informatiques » (fraude informatique, sabotage physique, attaque logique ciblée, divulgations, actes de chantage ou d'extorsion) ont été repérées dans moins d'un établissement sur 10.
 - © Forte diminution des vols avec 27% d'établissements concernés en 2018 contre 37% en 2014 et 44% en 2010.
 - © « perte de services essentiels » est en diminution forte à 17% (34% en 2014 et 46% en 2010)
-  © Dépôts de plainte faibles (de 4% à 11% en 4 ans)
-  © Peu de signalement des incidents graves sur « Portail de signalement des évènements sanitaires indésirables »

Gestion des incidents

© Confrontation avec les sujets du Panorama de la Cybercriminalité du CLUSIF :

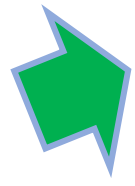
- Le Phishing est le sujet majeur auxquels les établissements de santé sont confrontés
- Les impacts constatés sont cependant faibles



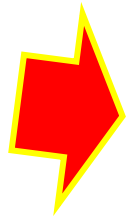
© Impact financier des incidents

- Peu d'établissements (1/3) font une analyse de l'impact financier des incidents
- Peu établissements (1/4) ont conduit une démarche d'analyse de la valeur des informations potentiellement perdues, altérées ou volées à travers la souscription d'une police d'assurance

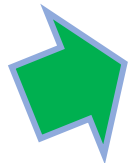
Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité



Un net développement de la mise en place de dispositifs de gestion de crise



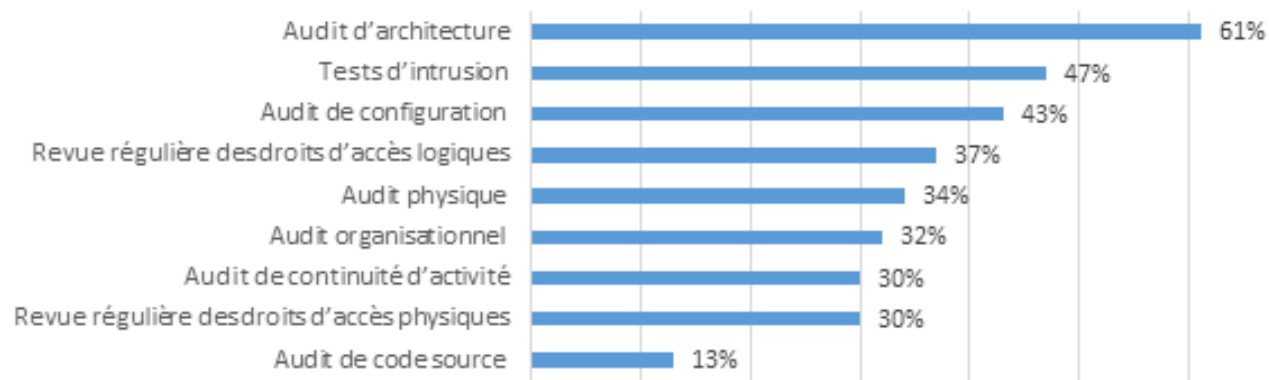
L'indisponibilité d'un fournisseur essentiel parent pauvre de la gestion de la continuité d'activité.



Fréquence des tests de plans de continuité en progression

Une conformité aux obligations légales et réglementaires en phase de consolidation

- © 67% des établissements sont soumis à des lois et/ou des règlements spécifiques
- © plus de 8 établissements sur 10 conformes aux exigences du Programme Hôpital Numérique
- © 56% des établissements sont prêts pour le Règlement Général sur la Protection des Données (RGPD)
- © La responsabilité de déclarer les traitements assurée au 2/3 par le RSSI et le CIL
- © 38% des établissements ont mis en place des tableaux de bord
- © Un fort développement des audits



En synthèse...



- © Tous les établissements ont des politiques de sécurité et répondent à des exigences réglementaires
- © Des ressources ciblées pour mettre en œuvre ces PSSI (équipe RSSI, cellule incidents et crise)
- © Meilleure connaissance du SI : L'inventaire des actifs
- © Meilleure connaissance des Risques : L'audit et inventaire des risques en progression forte
- © Plus de procédures : Gestion départs, tests PRA/PCA, gestion de crise
- © Actions de sensibilisation en croissance
- © Des plans de réduction des risques efficaces : diminution de la sinistralité
- © Des budgets en croissance mais mal identifiés et insuffisants
- © Les usages en mobilité sont de + en + surveillés
- © Les évolutions induites par GHT, RGPD : externalisation, mutualisation