CENTRE HOSPITALIER UNIVERSITAIRE DE NANTES

Approche du risque SI dans le monde de la santé

Le CHU de NANTES

7ème CHU de France, premier employeur de la région Pays de Loire

Mission de soins, d'enseignement et de recherche

7 sites principaux dans le court séjour (MCO), le long séjour (SSR) et la psychiatrie

Capacité d'accueil : 3 049 lits et places

Activité de soins (chiffres 2010)

800 000 entrées par an, 101 000 passages aux urgences (dont 29 000 pédiatriques)

439 000 appels au centre 15

Effectifs : 11 211 agents (8 869 non médicaux, 2 342 médicaux), plus de 12 000 en comptant les personnels sous convention

Projet de reconstruction du site principal à horizon 2020

Budget global : 726 M €

Présentation de l'intervenant

Cédric Cartau, RSSI du CHU de NANTES depuis 2009

A travaillé au CHU de REIMS et au CHU de RENNES

Membre de l'APSSIS, ARCSI, CESIN, AFCDP

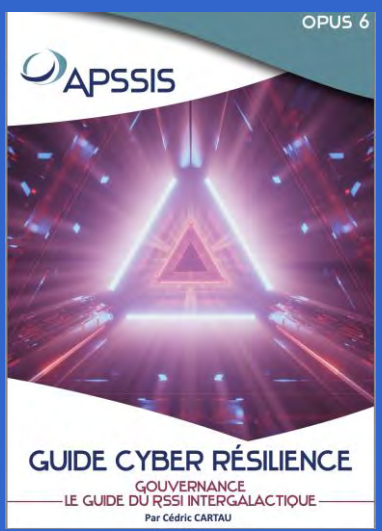
Chroniqueur dans DSIH Magazine

Auteur de 6 ouvrages spécialisés

Publication de 6 opus cyber résilience avec l'APSSIS

Enseignant à l'EHESP, ESIEA, Université de Nantes, CNEH

Jingle Publicité

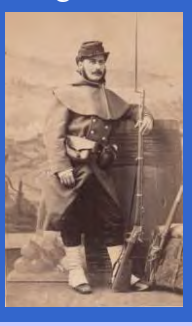


Avec WELIOM, MIPIH, WALLIX

Guest Star :

Philippe LOUDENOT (photo de 70)

Marguerite BRAC DE LA PERRIERE



1- HISTOIRE DES SI DE SANTE (SIS)

Avant 2000

Le tryptique RH / FACTU / GEF

Les CRIH

L'activité de développement interne

A partir de 2004

Plan HN / DOUSTE BLAZY

La stratégie progiciel

A partir de 2017

GHT

2- ETAT DES LIEUX DES SIS EN 2023

Echelle de notation : HIMSS (0 - 7)

Echelle budgétaire : études Européennes

Résultats :

- HIMSS : entre 3 et 4, aucun ES au niveau 6
- Budgets SI : en moyenne 1,7 % de l'OPEX

Ambitions nationales : HIMSS 6, aucun ES Européen à ce niveau avec moins de 3,5 % du budget SI

Budgets SSI : aucune mesure à ce jour, aucune échelle consensuelle

3 – LES ENJEUX SIS

- Cloudisation de l'informatique de santé : prise de RDV en ligne, DP accessible en direct, etc.
- Explosion des coûts : EDS, génomique, aide à la décision
- Les enjeux sociétaux : EDS, génomique, self quantifying, télémédecine
- Les enjeux métier

4 – LES TENDANCES SIS

- Tendance 1 : vers HIMSS L7
- Tendance 2 : le Big Data
- Tendance 3 : les centres de calcul
  - Vers la notion de clinique des données, de consultation des données d'ambulatoire des données
- Tendance 4 : IoT
- Tendance 5 : technicisation des actes médicaux
  - En 2030 les chirurgiens n'opèreront plus avec leurs mains
- Tendance 6 : prothèses, humains augmentés, capteurs, pilules connectées, etc.
  - Explosion des DM

4 – LES TENDANCES SIS

- Tendance 7 : BYOD massif
- Tendance 8 : ouverture massive des DPI
- Tendance 9 : les nouveaux matériaux
  - Impression 3D
  - matériaux composites et nanomatériaux
- Tendance 10 : les infrastructures de nouvelles génération
  - Infrastructures réparties internes / Cloud
- Tendance 11 : modifications structurelles profondes dans le financement des actes médicaux
  - Quel financement pour le bien-être ?
  - Ex : chirurgie esthétique
- Tendance 12 : vers la certification comme centre de gravité

5 – SPECIFICITE DU RISQUE SSI SANTE

- DICP, comme partout ailleurs
  - L'illusion du risque extrême dans le monde de la santé
- I, devant toujours
- D, second toujours
- C, dernier sauf exceptions
  - Quelles exceptions ?
- P, jamais sauf…

Quelques exemples

- L'identito vigilance ou le paroxysme du « I »
  - Les jumeaux facétieux ou le risque à tous les étages
  - Fusions, défusions
- SAMU, gestion des greffes et monitoring patients pour le « D »
- Hospitalisations sous X, hyperconfidentialité pour le « C »
- Traçabilité réglementaire pour le « P »

Quelques exemples

- Les contraintes de durées de conservation
  - Le RGPD et le droit à l'oubli
  - Les Code de la Santé Publique pour les durées de conservation
  - Les contraintes des Archives Départementales
- Les spécificités RGPD
  - Pas de droit d'opposition
  - Pas de droit d'effacement
  - Pas de droit de rectification

6 – ETAT DES LIEUX SSI

- Les enjeux de GHT : vers le DPI partagés à contraintes DIC fortement hétérogènes
- Les enjeux réglementaires : contraintes inhérentes à la Recherche médicale, HDS (et variabilité des interprétations de l'application HDS à la Recherche et aux GHT), CAC, NIS, RGPD, etc.
  - Avalanche de loi / décrets / arrêtés depuis 2017
- Les enjeux d'infrastructure : forte croissance des datacenters depuis 10 ans
- Les enjeux cyber

6 – ETAT DES LIEUX SSI

- Quelques exemples qui piquent très fort
  - Les VPN Lan To Lan
  - Les Windows 2000 encore présent
  - Les équipements sans AV ni patch OS...et pas que du biomed
  - Les liens direct de LAN à LAN sans FW
  - Les comptes admin de domaines distribués en goodies
  - Les types qui ramènent leur Box ADSL pour dédoubler les prises RJ45

6 – ETAT DES LIEUX SSI

- Quelques exemples qui piquent très fort
  - Le matos prêté par des labo...avec du Conficker Inside
  - Les WIFI Patients...sur le même SSID que le WIFI de production
  - Les associations « inside » qui pratiquent la stratégie du coucou
  - Les stagiaires qui ont plus de droit sur le DPI que le PU-PH
  - Les Géo Trouvetou qui trouve que c'est une bonne idée d'envoyer les prescriptions médoc par SMS
  - Les éditeurs qui livrent des applis Web pour lesquelles les utilisateurs doivent avoir un accès CT sur un partage de fichiers du serveur

6 – ETAT DES LIEUX SSI

- Quelques exemples qui piquent très fort
  - Les demande d'ouverture de flux en shunt du proxy / Firewall depuis un PC vers un serveur Internet sans filtrage de port

6 – ETAT DES LIEUX SSI

- Contexte cyber mondial et national
- Prise en compte récente dans les CH / CHU
- Les grandes « affaires » : ROUEN (2019-12), DAX (2021-04), VILLEFRANCHE, CORBEILLE, VERSAILLES

7 – ANALYSE DE LA SITUATION

Comment en est-on arrivés là, analyse structurelle et conjoncturelle

- Informatisation du coeur de métier, changement de paradigme DIC
- Déplacement constant de la dette : temporel et spatial
- Course en avant sur l'extension périmétrique du SI
- Difficultés réelles pour des décideurs d'intégrer dans les raisonnements les notions d'obsolescence et surtout d'obsolescence de la pile OSI
- Mélanges de métiers à contraintes DIC très diverses
- Arrivée d'un black swan : les ransomewares

7 – ANALYSE DE LA SITUATION

- Ecosystème fournisseur très hétérogène, le meilleur côtoie le pire
  - Et le pire devrait tout simplement être interdit d'exercer...
- Systèmes SCADA généralisés, choc de 2 mondes
- Problèmes de moyens, à la fois RH et Fi, à la fois RUN et BUILD
  - Les ambitions démesurées face aux moyens : HIMMS niveau 6 en ligne de mire alors que les budgets sont à peine ceux de HIMMS niveau 3
- DSI très en retard sur le sujet de la Qualité

8 – PROSPECTIVES SSI-S

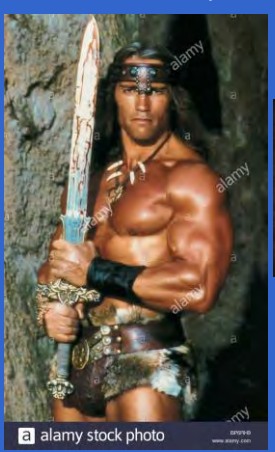
- Vers la certification : ITIL, ISO 27001
- Mesures techniques : Zero Trust généralisé, segmentation des réseaux, identification des pans du SI non essentiels susceptibles d'être définitivement éteints solutions mixtes On-Premise/Cloud, découpages en mode Ring 3 des architectures internes, réingénierie et automatisation au moins partielle du référentiel de contrôle, 2FA, voire 3FA
- Mesures formation : DH, intervention en amont dans les cursus médico-soignants, passeport SSI interne, formation des DSI
- Utilisation de la BlockChain en santé : usages et limites

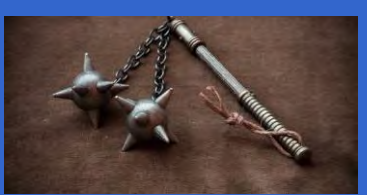
8 – PROSPECTIVES SSI-S

- Le cas de la génomique
  - Casse tous les paradigmes « C »
  - Fait exploser les budgets IT et SSI
  - Rend obsolète les matrices d'habilitation
  - Impacte la dimension sociétale
- Les points d'attention / danger
  - Vers une DSI « RSSI-centrée » / CHU « cyber-centré »

LE QUART D'HEURE PHILO

- Le RSSI reste en conseil et alerte, de l'importance de la négociation





9 – Les pistes de solution

Les points qui font consensus

- ❑ Réduire les flux de projet
- ❑ Réduire la voilure du SI
- ❑ Augmenter les moyens OPEX

Les points qui font débat

- ❑ Stopper les financements externes CAPEX
- ❑ Menaces cyber sans fin ni solution, envisager la scission d'Internet
- ❑ Prise en compte des archi Internet au niveau étatique

Conclusion

A quoi reconnait-on un SI mature sur la plan de la sécurité ?

- ■ A l'existence d'un processus d'évaluation
  - ✓ De l'utilisation de l'échelle COBIT
  - ✓ De l'appréciation de la maturité PDCA
  - ✓ D'une certification ISO : ITIL, 27001
- ■ A la notion de « voiture-balais »
- ■ A l'intégration de la SSI dans la prise de décision top-management

Citation

« On obtient plus de choses en étant poli et armé qu'en étant simplement poli »

Al Capone

Bibliographie et sites internet

- « La sécurité du système d'information des établissements de santé », Cédric Cartau, Presses de l'EHESP, mai 2012
- Tous les cyber guide publiés à l'APSSIS
- « Guide pratique du système d'information », Cédric Cartau, Presses de l'EHESP, mai 2013
- « Les décisions absurdes I et II », Christian MOREL
- « Management de la sécurité du SI », Alexandre Fernandez-Toro

Questions / réponses
Mais avant la parole est à...

Publications